

EXHIBIT 12

Screening Out Family Time:
The For-Profit Video Visitation Industry in Prisons and Jails

Maricopa County, Arizona Securus Contract and Proposal

PRISON
POLICY INITIATIVE

SERIAL 13002-RFP WEB-BASED VISITATION/COMMUNICATION KIOSK SYSTEM

DATE OF LAST REVISION: November 06, 2013

CONTRACT END DATE: November 30, 2018

CONTRACT PERIOD THROUGH NOVEMBER 30, 2018

TO: All Departments

FROM: Office of Procurement Services

SUBJECT: Contract for **WEB-BASED VISITATION/COMMUNICATION KIOSK SYSTEM**

Attached to this letter is published an effective purchasing contract for products and/or services to be supplied to Maricopa County activities as awarded by Maricopa County on **November 06, 2013**.

All purchases of products and/or services listed on the attached pages of this letter are to be obtained from the vendor holding the contract. Individuals are responsible to the vendor for purchases made outside of contracts. The contract period is indicated above.

Wes Baysinger, Chief Procurement Officer
Office of Procurement Services

JG/mm
Attach

Copy to: Office of Procurement Services
Sue Malinowski, MCSO
Amie Bristol, MCSO



CONTRACT PURSUANT TO RFP

SERIAL 13002-RFP

This Contract is entered into this 6th day of November, 2013 by and between Maricopa County ("County"), a political subdivision of the State of Arizona, and Securus Technologies, Inc., a Texas corporation ("Contractor") for the installation of Web-Based Video Visitation equipment, services, support and Kiosk Based services that will create a revenue sharing program between the Parties.

1.0 CONTRACT TERM:

- 1.1 This Contract is for a term of five (5) years, beginning on the 6th day of November, 2013 and ending the 30th day of November, 2018.
- 1.2 The County may, at its option and with the agreement of the Contractor, renew the term of this Contract for additional terms up to a maximum of ten (10) years, (or at the County's sole discretion, extend the contract on a month-to-month bases for a maximum of six (6) months after expiration). The County shall notify the Contractor in writing of its intent to extend the Contract term at least thirty (30) calendar days prior to the expiration of the original contract term, or any additional term thereafter.

2.0 REVENUE AND RATE ADJUSTMENTS:

- 2.1 The revenue share plan as detailed in Exhibit "A" shall remain in effect for the life of the Agreement unless a rate change is mutually agreed to in writing by the Parties.
- 2.2 The rate to be charged for visitation is defined in Exhibit "A". The rate and the designated customer groups to whom it applies shall be reviewed on a quarterly basis to ensure its fairness and reasonableness. Any changes to the rate shall be agreed to in writing by the Parties.

3.0 COMMISSION PAYMENTS AND ACCOUNTABILITY:

- 3.1 The commission offered to MCSO shall be based on total gross revenues (as outlined in the detailed pricing structure), with no deductions for fraud, bad debt, uncollectible, or un-billable calls. No deduction shall be made for any cost of providing the service(s) described.

- 3.2 Commissions shall be paid monthly and sent to:

Maricopa County Sheriff's Office
234 N. Central Avenue, 7th floor
Phoenix, AZ 85004
Attn: Financial Services Division

- 3.3 Payment shall arrive no later than thirty (30) days following the calendar month for which commissions are being paid. Failure to submit commissions within sixty (60) days following the billing month gives the County the right to impose and collect interest at the maximum legal rate for all late payments.

- 3.4 Failure to pay accurate commissions on a regular, monthly basis shall be grounds for cancellation, without penalty, of agreement executed as a result of the RFP.
- 3.5 A monthly commission and summary report that includes, at a minimum, the following information shall to be sent to the Web-based Video Visitation/Communication System Manager: date of report, time period covered, total number of calls by category, total number of minutes by category, total gross revenue (as defined above).

4.0 INVOICES AND PAYMENTS:

- 4.1 The Respondent shall submit two (2) legible copies of their detailed invoice before payment(s) can be made. At a minimum, the invoice must provide the following information:
 - Company name, address and contact
 - County bill-to name and contact information
 - Invoice number and date
 - Payment terms
 - Date of service or delivery
 - Quantity
 - Contract Item number(s)
 - Description of Purchase (services)
 - Pricing per unit of service
 - Extended price
 - Total Amount Due
- 4.2 Problems regarding billing or invoicing shall be directed to the using agency as listed on the Purchase Order
- 4.3 Payment shall be made to the Contractor by Accounts Payable through the Maricopa County Vendor Express Payment Program. This is an Electronic Funds Transfer (EFT) process. After Contract Award the Contractor shall complete the Vendor Registration Form located on the County Department of Finance Vendor Registration Web Site (www.maricopa.gov/finance/vendors).
- 4.4 EFT payments to the routing and account numbers designated by the Contractor will include the details on the specific invoices that the payment covers. The Contractor is required to discuss remittance delivery capabilities with their designated financial institution for access to those details.

5.0 STRATEGIC ALLIANCE for VOLUME EXPENDITURES (\$AVE):

- 5.1 The County is a member of the \$AVE cooperative purchasing group. \$AVE includes the State of Arizona, many Phoenix metropolitan area municipalities, and many K-12 unified school districts. Under the \$AVE Cooperative Purchasing Agreement, and with the concurrence of the successful Respondent under this solicitation, a member of \$AVE may access a contract resulting from a solicitation issued by the County. If you **do not** want to grant such access to a member of \$AVE, **please so state** in your proposal. In the absence of a statement to the contrary, the County will assume that you do wish to grant access to any contract that may result from this Request for Proposal.

6.0 INTERGOVERNMENTAL COOPERATIVE PURCHASING AGREEMENTS (ICPA's)

- 6.1 County currently holds ICPA's with numerous governmental entities throughout the State of Arizona. These agreements allow those entities, with the approval of the Contractor, to purchase their requirements under the terms and conditions of the County Contract. Please indicate on Attachment A, your acceptance or rejection regarding such participation of other governmental entities. Your response will not be considered as an evaluation factor in awarding a contract

7.0 AVAILABILITY OF FUNDS:

- 7.1 The provisions of this Contract relating to payment for services shall become effective when funds assigned for the purpose of compensating the Contractor as herein provided are actually available to County for disbursement. The County shall be the sole judge and authority in determining the availability of funds under this Contract. County shall keep the Contractor fully informed as to the availability of funds.
- 7.2 If any action is taken by any state agency, Federal department or any other agency or instrumentality to suspend, decrease, or terminate its fiscal obligations under, or in connection with, this Contract, County may amend, suspend, decrease, or terminate its obligations under, or in connection with, this Contract. In the event of termination, County shall be liable for payment only for services rendered prior to the effective date of the termination, provided that such services are performed in accordance with the provisions of this Contract. County shall give written notice of the effective date of any suspension, amendment, or termination under this Section, at least ten (10) days in advance.

8.0 DUTIES:

- 8.1 The Contractor shall perform all duties stated in Exhibit "B", or as otherwise directed in writing by the Procurement Officer. If any questions arise regarding the stated requirements, both MCSO and vendor agree to work toward a mutually agreeable solution.
- 8.2 During the Contract term, County shall provide Contractor's personnel with adequate workspace for consultants and such other related facilities as may be required by Contractor to carry out its contractual obligations.

9.0 TERMS and CONDITIONS:

9.1 INDEMNIFICATION:

- 9.1.1 To the fullest extent permitted by law, Contractor shall defend, indemnify, and hold harmless County, its agents, representatives, officers, directors, officials, and employees from and against all claims, damages, losses and expenses, including, but not limited to, attorney fees, court costs, expert witness fees, and the cost of appellate proceedings, relating to, arising out of, or alleged to have resulted from the negligent acts, errors, omissions, mistakes or malfeasance relating to the performance of this Contract. Contractor's duty to defend, indemnify and hold harmless County, its agents, representatives, officers, directors, officials, and employees shall arise in connection with any claim, damage, loss or expense that is caused by any negligent acts, errors, omissions or mistakes in the performance of this Contract by the Contractor, as well as any person or entity for whose acts, errors, omissions, mistakes or malfeasance Contractor may be legally liable.
- 9.1.2 The amount and type of insurance coverage requirements set forth herein will in no way be construed as limiting the scope of the indemnity in this paragraph.

The scope of this indemnification does not extend to the sole negligence of County

9.2 INSURANCE:

- 9.2.1 Contractor, at Contractor's own expense, shall purchase and maintain the herein stipulated minimum insurance from a company or companies duly licensed by the State of Arizona and possessing a current A.M. Best, Inc. rating of A+. In lieu of State of Arizona licensing, the stipulated insurance may be purchased from a company or companies, which are authorized to do business in the State of Arizona, provided that said insurance companies meet the approval of County. The form of any insurance policies and forms must be acceptable to County.

- 9.2.2 All insurance required herein shall be maintained in full force and effect until all work or service required to be performed under the terms of the Contract is satisfactorily completed and formally accepted. Failure to do so may, at the sole discretion of County, constitute a material breach of this Contract.
- 9.2.3 Contractor's insurance shall be primary insurance as respects County, and any insurance or self-insurance maintained by County shall not contribute to it.
- 9.2.4 Any failure to comply with the claim reporting provisions of the insurance policies or any breach of an insurance policy warranty shall not affect the County's right to coverage afforded under the insurance policies.
- 9.2.5 The insurance policies may provide coverage that contains deductibles or self-insured retentions. Such deductible and/or self-insured retentions shall not be applicable with respect to the coverage provided to County under such policies. Contractor shall be solely responsible for the deductible and/or self-insured retention and County, at its option, may require Contractor to secure payment of such deductibles or self-insured retentions by a surety bond or an irrevocable and unconditional letter of credit.
- 9.2.6 County reserves the right to request and to receive, within 10 working days, certified copies of any or all of the herein required insurance certificates. County shall not be obligated to review policies and/or endorsements or to advise Contractor of any deficiencies in such policies and endorsements, and such receipt shall not relieve Contractor from, or be deemed a waiver of County's right to insist on strict fulfillment of Contractor's obligations under this Contract.
- 9.2.7 The insurance policies required by this Contract, except Workers' Compensation, shall name County, its agents, representatives, officers, directors, officials and employees as Additional Insureds.
- 9.2.8 The policies required hereunder, except Workers' Compensation, shall contain a waiver of transfer of rights of recovery (subrogation) against County, its agents, representatives, officers, directors, officials and employees for any claims arising out of Contractor's work or service.
- 9.2.9 Commercial General Liability:

Commercial General Liability insurance and, if necessary, Commercial Umbrella insurance with a limit of not less than \$2,000,000 for each occurrence, \$2,000,000 Products/Completed Operations Aggregate, and \$4,000,000 General Aggregate Limit. The policy shall include coverage for bodily injury, broad form property damage, personal injury, products and completed operations and blanket contractual coverage, and shall not contain any provision which would serve to limit third party action over claims. There shall be no endorsement or modification of the CGL limiting the scope of coverage for liability arising from explosion, collapse, or underground property damage.
- 9.2.10 Automobile Liability:

Commercial/Business Automobile Liability insurance and, if necessary, Commercial Umbrella insurance with a combined single limit for bodily injury and property damage of not less than \$2,000,000 each occurrence with respect to any of the Contractor's owned, hired, and non-owned vehicles assigned to or used in performance of the Contractor's work or services under this Contract.
- 9.2.11 Workers' Compensation:
 - 9.2.11.1 Workers' Compensation insurance to cover obligations imposed by federal and state statutes having jurisdiction of Contractor's employees engaged in the performance of the work or services under this Contract; and Employer's

Liability insurance of not less than \$1,000,000 for each accident, \$1,000,000 disease for each employee, and \$1,000,000 disease policy limit.

- 9.2.11.2 Contractor waives all rights against County and its agents, officers, directors and employees for recovery of damages to the extent these damages are covered by the Workers' Compensation and Employer's Liability or commercial umbrella liability insurance obtained by Contractor pursuant to this Contract.

9.2.12 Certificates of Insurance.

- 9.2.12.1 Prior to commencing work or services under this Contract, Contractor shall have insurance in effect as required by the Contract in the form provided by the County, issued by Contractor's insurer(s), as evidence that policies providing the required coverage, conditions and limits required by this Contract are in full force and effect. Such certificates shall be made available to the County upon ten (10) business days. **BY SIGNING THE AGREEMENT PAGE THE CONTRACTOR AGREES TO THIS REQUIREMENT AND FAILURE TO MEET THIS REQUIREMENT WILL RESULT IN CANCELLATION OF CONTRACT.**

- 9.2.12.1.1 In the event any insurance policy (ies) required by this contract is (are) written on a "claims made" basis, coverage shall extend for two years past completion and acceptance of Contractor's work or services and as evidenced by annual Certificates of Insurance.

- 9.2.12.1.2 If a policy does expire during the life of the Contract, a renewal certificate must be sent to County fifteen (15) days prior to the expiration date.

9.2.13 Cancellation and Expiration Notice.

Insurance required herein shall not be permitted to expire, be canceled, or materially changed without thirty (30) days prior written notice to the County.

9.3 WARRANTY OF SERVICES:

- 9.3.1 The Contractor warrants that all services provided hereunder will conform to the requirements of the Contract, including all descriptions, specifications and attachments made a part of this Contract. County's acceptance of services or goods provided by the Contractor shall not relieve the Contractor from its obligations under this warranty.
- 9.3.2 In addition to its other remedies, County may, at the Contractor's expense, require prompt correction of any services failing to meet the Contractor's warranty herein. Services corrected by the Contractor shall be subject to all the provisions of this Contract in the manner and to the same extent as services originally furnished hereunder.

9.4 INSPECTION OF SERVICES:

- 9.4.1 The Contractor shall provide and maintain an inspection system acceptable to County covering the services under this Contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to County during contract performance and for as long afterwards as the Contract requires.
- 9.4.2 County has the right to inspect and test all services called for by the Contract, to the extent practicable at all times and places during the term of the Contract. County shall perform inspections and tests in a manner that will not unduly delay the work.

9.4.3 If any of the services do not conform with the Contract requirements, County may require the Contractor to perform the services again in conformity with Contract requirements, at no increase in Contract amount. When the defects in services cannot be corrected by re-performance, County may:

9.4.3.1 Require the Contractor to take necessary action to ensure that future performance conforms to Contract requirements; and

9.4.3.2 Reduce the Contract price to reflect the reduced value of the services performed.

9.4.4 If the Contractor fails to promptly perform the services again or to take the necessary action to ensure future performance in conformity with Contract requirements, County may:

9.4.4.1 By Contract or otherwise, perform the services and charge to the Contractor any cost incurred by County that is directly related to the performance of such service; or

9.4.4.2 Terminate the Contract for default.

9.5 NOTICES:

All notices given pursuant to the terms of this Contract shall be addressed to:

For County:

Maricopa County
Office of Procurement Services
ATTN: Contract Administration
320 West Lincoln Street
Phoenix, Arizona 85003-2494

For Contractor:

Securus Technologies
Attn: General Counsel
14651 Dallas Parkway
Suite 600
Dallas, TX 75254

9.6 REQUIREMENTS CONTRACT:

9.6.1 Contractor signifies its understanding and agreement by signing this document that this Contract is a requirements contract. This Contract does not guarantee any purchases will be made (minimum or maximum). Orders will only be placed when County identifies a need and issues a purchase order or a written notice to proceed.

9.6.2 County reserves the right to cancel purchase orders or notice to proceed within a reasonable period of time after issuance. Should a purchase order or notice to proceed be canceled, the County agrees to reimburse the Contractor for actual and documented costs incurred by the Contractor. The County will not reimburse the Contractor for any avoidable costs incurred after receipt of cancellation, or for lost profits, or shipment of product or performance of services prior to issuance of a purchase order or notice to proceed.

9.6.3 Purchase orders will be cancelled in writing.

9.7 TERMINATION FOR CONVENIENCE:

The County reserves the right to terminate the Contract, in whole or in part at any time, when in the best interests of the County without penalty or recourse. Upon receipt of the written notice, the Contractor shall immediately stop all work, as directed in the notice, notify all subcontractors of the effective date of the termination and minimize all further costs to the County. In the event of termination under this paragraph, all documents, data and reports prepared by the Contractor under the Contract shall become the property of and be delivered to the County upon demand. The Contractor shall be entitled to receive just and equitable compensation for work in progress, work completed and materials accepted before the effective date of the termination. If the Agreement is terminated for any reason before the end of the Initial Term, Customer will refund to Contractor the prorated amount of the Video Visitation system \$2,603,201.95. County shall pay any such refund within thirty (30) days after any such termination, or at Contractor's election, Contractor may deduct the refund from any commission owed to County.

9.8 TERMINATION FOR DEFAULT:

9.8.1 In addition to the rights reserved in the Contract, the County may terminate the Contract in whole or in part due to the failure of the Contractor to comply with any term or condition of the Contract, to acquire and maintain all required insurance policies, bonds, licenses and permits, or to make satisfactory progress in performing the Contract. The Procurement Officer shall provide written notice of the termination and the reasons for it to the Contractor. Prior to any such notice of termination, County shall provide Contractor a notice of alleged breach(es), setting forth all concerns with specificity, and providing Contractor with a cure schedule that is of a length appropriate to the breach. In the event of willful misconduct or negligence on the part of the Contractor, no cure shall be offered and termination shall be immediate. Cure schedules for system performance breaches shall be aligned with the service levels detailed in Section 4.5 of Exhibit B.

9.8.2 Upon termination under this paragraph, all goods, materials, documents, data and reports prepared by the Contractor under the Contract shall become the property of and be delivered to the County on demand.

9.8.3 The County may, upon termination of this Contract, procure, on terms and in the manner that it deems appropriate, materials or services to replace those under this Contract. The Contractor shall be liable to the County for any excess costs incurred by the County in procuring materials or services in substitution for those due from the Contractor.

9.8.4 The Contractor shall continue to perform, in accordance with the requirements of the Contract, up to the date of termination, as directed in the termination notice.

9.9 TERMINATION BY THE COUNTY:

If the Contractor should be adjudged bankrupt or should make a general assignment for the benefit of its creditors, or if a receiver should be appointed on account of its insolvency, the County may terminate the Contract. If the Contractor should persistently or repeatedly refuse or should fail, except in cases for which extension of time is provided, to provide enough properly skilled workers or proper materials, or persistently disregard laws and ordinances, or not proceed with work or otherwise be guilty of a substantial violation of any provision of this Contract, then the County may terminate the Contract. Prior to termination of the Contract, the County shall give the Contractor fifteen- (15) calendar day's written notice. Upon receipt of such termination notice, the Contractor shall be allowed fifteen (15) calendar days to cure such deficiencies.

9.10 STATUTORY RIGHT OF CANCELLATION FOR CONFLICT OF INTEREST:

Notice is given that pursuant to A.R.S. §38-511 the County may cancel this Contract without penalty or further obligation within three years after execution of the contract, if any person significantly involved in initiating, negotiating, securing, drafting or creating the contract on behalf of the County is at any time while the Contract or any extension of the Contract is in effect,

an employee or agent of any other party to the Contract in any capacity or consultant to any other party of the Contract with respect to the subject matter of the Contract. Additionally, pursuant to A.R.S §38-511 the County may recoup any fee or commission paid or due to any person significantly involved in initiating, negotiating, securing, drafting or creating the contract on behalf of the County from any other party to the contract arising as the result of the Contract.

9.11 OFFSET FOR DAMAGES;

In addition to all other remedies at law or equity, the County may offset from any money due to the Contractor any amounts Contractor owes to the County for damages resulting from breach or deficiencies in performance under this contract.

9.12 ADDITIONS/DELETIONS OF SERVICE:

9.12.1 The County reserves the right to add and/or delete materials to a Contract. If a service requirement is added or deleted, payment or reductions to the Contractor will be negotiated between the Contractor and the County.

9.12.2 The County reserves the right of final approval on proposed staff for all Task Orders. Also, upon request by the County, the Contractor will be required to remove any employees working on County projects and substitute personnel based on the discretion of the County within two business days, unless previously approved by the County.

9.13 RELATIONSHIPS:

In the performance of the services described herein, the Contractor shall act solely as an independent contractor, and nothing herein or implied herein shall at any time be construed as to create the relationship of employer and employee, partnership, principal and agent, or joint venture between the District and the Contractor.

9.14 SUBCONTRACTING:

The Contractor may not assign this Contract or subcontract to another party for performance of the terms and conditions hereof without the written consent of the County, which shall not be unreasonably withheld. All correspondence authorizing subcontracting must reference the Proposal Serial Number and identify the job project.

9.15 AMENDMENTS:

All amendments to this Contract shall be in writing and approved/signed by both parties. Maricopa County Office of Procurement Services shall be responsible for approving all amendments for Maricopa County.

9.16 ACCESS TO AND RETENTION OF RECORDS FOR THE PURPOSE OF AUDIT AND/OR OTHER REVIEW:

9.16.1 In accordance with section MCI 371 of the Maricopa County Procurement Code the Contractor agrees to retain all books, records, accounts, statements, reports, files, and other records and back-up documentation relevant to this Contract for six (6) years after final payment or until after the resolution of any audit questions which could be more than six (6) years, whichever is latest. The County, Federal or State auditors and any other persons duly authorized by the Department shall have full access to, and the right to examine, copy and make use of, any and all said materials.

9.16.2 If the Contractor's books, records, accounts, statements, reports, files, and other records and back-up documentation relevant to this Contract are not sufficient to support and document that requested services were provided, the Contractor shall reimburse Maricopa County for the services not so adequately supported and documented.

9.16.3 If at any time it is determined by the County that a cost for which payment has been made is a disallowed cost, the County shall notify the Contractor in writing of the disallowance. The course of action to address the disallowance shall be at sole discretion of the County, and may include either an adjustment to future claim submitted by the Contractor by the amount of the disallowance, or to require reimbursement forthwith of the disallowed amount by the Contractor by issuing a check payable to Maricopa County.

9.17 AUDIT DISALLOWANCES:

If at any time, County determines that a cost for which payment has been made is a disallowed cost, such as overpayment, County shall notify the Contractor in writing of the disallowance. County shall also state the means of correction, which may be but shall not be limited to adjustment of any future claim submitted by the Contractor by the amount of the disallowance, or to require repayment of the disallowed amount by the Contractor.

9.18 SEVERABILITY:

The invalidity, in whole or in part, of any provision of this Contract shall not void or affect the validity of any other provision of this Contract.

9.19 RIGHTS IN DATA:

The County shall own have the use of all data and reports resulting from this Contract without additional cost or other restriction except as provided by law. Each party shall supply to the other party, upon request, any available information that is relevant to this Contract and to the performance hereunder.

9.20 INTEGRATION:

This Contract represents the entire and integrated agreement between the parties and supersedes all prior negotiations, proposals, communications, understandings, representations, or agreements, whether oral or written, express or implied.

9.21 VERIFICATION REGARDING COMPLIANCE WITH ARIZONA REVISED STATUTES §41-4401 AND FEDERAL IMMIGRATION LAWS AND REGULATIONS:

9.21.1 By entering into the Contract, the Contractor warrants compliance with the Immigration and Nationality Act (INA using e-verify) and all other federal immigration laws and regulations related to the immigration status of its employees and A.R.S. §23-214(A). The contractor shall obtain statements from its subcontractors certifying compliance and shall furnish the statements to the Procurement Officer upon request. These warranties shall remain in effect through the term of the Contract. The Contractor and its subcontractors shall also maintain Employment Eligibility Verification forms (I-9) as required by the Immigration Reform and Control Act of 1986, as amended from time to time, for all employees performing work under the Contract and verify employee compliance using the E-verify system and shall keep a record of the verification for the duration of the employee's employment or at least three years, whichever is longer. I-9 forms are available for download at USCIS.GOV.

9.21.2 The County retains the legal right to inspect contractor and subcontractor employee documents performing work under this Contract to verify compliance with paragraph 9.21.1 of this Section. Contractor and subcontractor shall be given reasonable notice of the County's intent to inspect and shall make the documents available at the time and date specified. Should the County suspect or find that the Contractor or any of its subcontractors are not in compliance, the County will consider this a material breach of the contract and may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

9.22 CONTRACTOR LICENSE REQUIREMENT:

- 9.22.1 The Respondent shall procure all permits, insurance, licenses and pay the charges and fees necessary and incidental to the lawful conduct of his/her business, and as necessary complete any required certification requirements, required by any and all governmental or non-governmental entities as mandated to maintain compliance with and in good standing for all permits and/or licenses. The Respondent shall keep fully informed of existing and future trade or industry requirements, Federal, State and Local laws, ordinances, and regulations which in any manner affect the fulfillment of a Contract and shall comply with the same. Contractor shall immediately notify both Office of Procurement Services and the using agency of any and all changes concerning permits, insurance or licenses.
- 9.22.2 Respondents furnishing finished products, materials or articles of merchandise that will require installation or attachment as part of the Contract, shall possess any licenses required. A Respondent is not relieved of its obligation to possess the required licenses by subcontracting of the labor portion of the Contract. Respondents are advised to contact the Arizona Registrar of Contractors, Chief of Licensing, at (602) 542-1525 to ascertain licensing requirements for a particular contract. Respondents shall identify which license(s), if any, the Registrar of Contractors requires for performance of the Contract.

9.23 CERTIFICATION REGARDING DEBARMENT AND SUSPENSION

- 9.23.1 The undersigned (authorized official signing for the Contractor) certifies to the best of his or her knowledge and belief, that the Contractor, defined as the primary participant in accordance with 45 CFR Part 76, and its principals:
 - 9.24.1.1 are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal Department or agency;
 - 9.24.1.2 have not within 3-year period preceding this Contract been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
 - 9.24.1.3 are not presently indicted or otherwise criminally or civilly charged by a government entity (Federal, State or local) with commission of any of the offenses enumerated in paragraph (2) of this certification; and
 - 9.24.1.4 have not within a 3-year period preceding this Contract had one or more public transaction (Federal, State or local) terminated for cause of default.
- 9.23.2 Should the Contractor not be able to provide this certification, an explanation as to why should be attached to the Contract.
- 9.23.3 The Contractor agrees to include, without modification, this clause in all lower tier covered transactions (i.e. transactions with subcontractors) and in all solicitations for lower tier covered transactions related to this Contract.

9.24 RATES:

Contractor warrants that rates extended to County under this Contract are no lower than those paid by any other customer for these or similar services.

9.25 GOVERNING LAW:

This Contract shall be governed by the laws of the state of Arizona. Venue for any actions or lawsuits involving this Contract will be in Maricopa County Superior Court or in the United States District Court for the District of Arizona, sitting in Phoenix, Arizona

9.26 ORDER OF PRECEDENCE:

In the event of a conflict in the provisions of this Contract and Contractor's license agreement, if applicable, the terms of this Contract shall prevail.

9.27 INFLUENCE

As prescribed in MC1-1202 of the Maricopa County Procurement Code, any effort to influence an employee or agent to breach the Maricopa County Ethical Code of Conduct or any ethical conduct, may be grounds for Disbarment or Suspension under MC1-902.

An attempt to influence includes, but is not limited to:

9.27.1 A Person offering or providing a gratuity, gift, tip, present, donation, money, entertainment or educational passes or tickets, or any type valuable contribution or subsidy,

9.27.2 That is offered or given with the intent to influence a decision, obtain a contract, garner favorable treatment, or gain favorable consideration of any kind.

If a Person attempts to influence any employee or agent of Maricopa County, the Chief Procurement Officer, or his designee, reserves the right to seek any remedy provided by the Maricopa County Procurement Code, any remedy in equity or in the law, or any remedy provided by this contract.

9.28 PUBLIC RECORDS:

All Offers submitted and opened are public records and must be retained by the Records Manager at the Office of Procurement Services. Offers shall be open to public inspection after Contract award and execution, except for such Offers deemed to be confidential by the Office of Procurement Services. If an Offeror believes that information in its Offer should remain confidential, it shall indicate as confidential, the specific information and submit a statement with its offer detailing the reasons that the information should not be disclosed. Such reasons shall include the specific harm or prejudice which may arise. The Records Manager of the Office of Procurement Services shall determine whether the identified information is confidential pursuant to the Maricopa County Procurement Code.

9.29 INCORPORATION OF DOCUMENTS:

The following are to be attached to and made part of this Contract:

9.29.1 Exhibit A, Pricing;

9.29.2 Exhibit B, Scope of Work;

9.29.3 Exhibit C, Code of Conduct Policy;

9.29.4 Exhibit D, Jail Access Policy;

9.29.5 Exhibit E, Inmate Visitation Policy;

9.29.6 Exhibit F, Current Video Visitation System Equipment

9.29.7 Exhibit G, POD Capacity Listing

- 9.29.8 Exhibit H, MCSO Security Guidelines
- 9.29.9 Exhibit I, OET Cabling Standards
- 9.29.10 Exhibit J, Implementation Schedule
- 9.29.11 Exhibit K, Hosting Requirements
- 9.29.12 Exhibit L, Minimum Kiosk Deployment Requirement

IN WITNESS WHEREOF, this Contract is executed on the date set forth above.

CONTRACTOR



AUTHORIZED SIGNATURE

Robert Pickens
PRINTED NAME AND TITLE

14651 Dallas Pkwy, Dallas, Tx 75254
ADDRESS

10-4-13
DATE

MARICOPA COUNTY


CHAIRMAN, BOARD OF SUPERVISORS


NOV 13 2013
DATE

ATTESTED:


CLERK OF THE BOARD 110613

NOV 13 2013
DATE

APPROVED AS TO FORM:


LEGAL COUNSEL

Nov 8 2013
DATE

EXHIBIT A**PRICING**

SERIAL 13002 - RFP

NIGP CODE: 83834

COMPANY NAME:

Securus Technologies, Inc

DOING BUSINESS AS (DBA) NAME:

Securus Technologies

MAILING ADDRESS:

14651 Dallas Parkway, Suite 600Dallas, TX 75254

REMIT TO ADDRESS:

Same

TELEPHONE NUMBER:

972-277-0300

FACSIMILE NUMBER:

972-277-0514

WEB SITE:

www.securustech.net

REPRESENTATIVE NAME:

Darrin Hays

REPRESENTATIVE PHONE NUMBER:

480-717-8790

REPRESENTATIVE E-MAIL:

dhays@securustech.net

WILL ALLOW OTHER GOVERNMENTAL ENTITIES TO PURCHASE FROM THIS
CONTRACT:

YES

PAYMENT TERMS: ☒ NET 30 DAYS**1.0 PROFIT SHARING:**

1.1 Base Rate for paid inmate visitation
\$12.95 for 20 minute session and up to or exceeding
\$40.00 as mutually agreed to by the parties. The
parties, by mutual written consent, may elect to offer
periodic price adjustments (Special Pricing) if deemed
necessary and appropriate. The consent shall detail the
adjusted rate, its intended purpose and its duration.

Contractor will provide the following at no cost to Maricopa County:

- 602 video visitation terminals (includes visitation centers and inmate terminals) as described in Exhibit "K"
- Software application setup — including JMS import mapping
- Video session recording storage — 60 days
- Video visitation software licensing fees
- On-site training on use of the visitation system
- Data network for video visitation traffic, but not including bandwidth required for County monitoring of the live or recorded visitations.

The cost for the following items shall be capped at \$879,000.00 unless mutually agreed to by the parties. This allowance is included within the stated ROI total in section titled Commissions.

- Wiring of your facilities with CAT6E cable via conduit were necessary
- A site inspection conducted by a qualified electrical engineer to determine appropriate electrical service is available to all proposed installation locations.
- All electrical cabling to each terminal

Contractor will provide the Cat6E cabling, required electrical to each terminal, the Inmate and Visitor Center visitation terminals, Internet bandwidth required, and ongoing support at no charge to Maricopa County.

Inmates will be allowed three (3) onsite visits per week, at no charge, for non-professional visitors, subject to lower modification (but in no case more than three (3) onsite visits per week) pursuant to policies of County. Contractor may charge visitation prices of up to \$20.00 per session for any additional onsite, non-professional visitations. County shall eliminate non-professional contact and non-contact visitation, and County shall use video visitation as the sole means to conduct non-professional visitation. In addition, all non-professional visitation, including on-site visitation, must be scheduled through Contractor's video visitation system.

County agrees that it shall seek to achieve one paid visit per inmate per month within six (6) months of implementation. County understands that, if this goal is not achieved, it will modify its operational processes, including but not limited to altering to the availability of onsite visitation or other recommendations provided by Contractor.

Contractor agrees to not charge for additional hardware refresh equipment beyond the initial deployment of 602 terminals.

Commissions

Contractor shall provide an initial revenue share of ten percent 10% of gross revenues per month upon implementation of the base Video Visitation System if the County reaches a minimum usage rate of 8,000 paid visits for the given month. Upon Contractor realizing \$2,603,201.95 in gross revenue, as verified by electronic tracking of visit usage times the visitation rate, the revenue percentage shall increase to twenty percent (20%) of gross revenue per month, regardless of visitation volume. The parties agree that the set commission rates shall be periodically reviewed in relation to the actual visitation volume and gross revenue and may be adjusted by mutual written consent.

EXHIBIT B**SCOPE OF WORK****1.0 INTENT:**

Maricopa County (hereafter referred to as County) requests your organization to submit a written proposal to enter into a revenue contract for providing a completely installed and functioning Internet-based remote video visitation and inmate communication kiosk system. Also, multiple distinct phases providing additional functionality are detailed in this document including: inmate email, ability to access policies and complete basic forms including, but not limited to, Inmate Request Forms, Inmate Grievances, Disciplinary Action Appeals, and Health Needs Request Forms. The system will also provide the ability to order from the MCSO Commissary. This would be an all-inclusive kiosk system that would allow Maricopa County Sheriff's Jails (hereafter referred to as MCSO) to go virtually paperless. The system must allow access from any location with Internet service.

Contractor shall provide a Video Visitation System (VVS) that is a fully Web-based video visitation platform and integrated inmate kiosk solution specifically designed for correctional facilities.

VVS shall enable Maricopa County to conduct visitations safely, securely, and with fewer burdens on facility staff. This advanced solution provides multiple benefits, including:

- Enhanced facility security by reducing the possibility of inmate confrontation
- Reduction in inmate and visitor movement through a facility
- Improved inmate ability to communicate with legal representation, bail-bond facilities, family, and any other persons authorized by Maricopa County Jail administration
- Reduction in contraband infiltration
- Increased security for visitors
- Increased inmate and visitor morale with increased opportunities to visit
- Reduced resources needed to escort inmates and visitors to visiting areas
- New revenue stream for the facility through paid visitation sessions

The VVS solution shall be a centralized system that will allow automatic technology and feature upgrades. VVS will enable inmates to order from the commissary as well as complete inmate requests and grievance forms using the terminal.

At-home or remote visitation sessions allow friends and family, bail bondsmen, probation officers, and attorneys to securely communicate with inmates from outside the facility via a broadband Internet connection. Because VVS is Internet-based, visitation sessions can be scheduled and conducted from any location with Internet services.

Remote visitors access Contractor Video Visitation through the www.securustech.net Web site. The visitor selects the facility and inmate they would like to visit. The visitor is able to do the following:

- Create, edit, and/or delete scheduled video sessions with inmates
- Pay for the scheduled session with a credit or debit card
- Visit with inmates (no officer intervention required)

Remote users will need to use a personal computer or laptop with a built-in or external USB Web camera, a microphone and speakers, or a headset.

Contractor shall provide VVS to Maricopa County, including installation and maintenance as well as personnel to operate and maintain the system at no cost to the County.

2.0 SCOPE OF WORK:

2.1 GENERAL REQUIREMENTS

Maricopa County is seeking a single Contractor with end-to-end responsibility for a turnkey inmate Web-based Video Visitation/Communication Kiosk System and services. Subcontractor relationships shall be permitted; however, the Contractor shall be responsible for the entire operation of the Web-based Video Visitation/Communication Kiosk system. The proposer shall verify the completeness of all service components and ensure that any and all equipment, materials and services required for installation, operation, or maintenance will be provided by proposer without claim for payment or reduction in commission level. Maricopa County shall bear no responsibility for any costs associated with the equipment and services solicited in the document. Solutions limited to point to point access will not be considered.

The Web-based Video Visitation/Communication Kiosk system must provide differentiation between legal and personal visits with a check and balance for the specific type of visit being requested, digital recording of personal visits made and a time synched network for all associated equipment in the system. The system must be of an open architecture to allow ease of integration with existing or future systems that operate on either PC based networks or mainframes. It must meet ADA requirements, provide access to both Spanish and English at the minimum, if not more, and have extensive IP address blocking capabilities at various levels and various times as deemed necessary by MCSO. The system shall be capable of downloading data to MCSO applications for investigative and statistical purposes and capable of receiving downloaded data from the Sheriff's Office Jail Management System or other MCSO systems. No third party/conference video chatting is permitted, unless specified by MCSO.

Contractor shall utilize as much competition as practical in the acquisition of goods and services for this Contract. County reserves the right to audit Contractor procurement practices, solicitations, contracts and orders directly related to the performance of the Contract.

Contractor shall only utilize County approved vendors for any sub-contracted work such as electrical installation. Contractor shall provide County a list of all proposed sub-contractors prior to implementation commencement. County reserves the right to dis-allow any sub-contractor for any reason with notice to Contractor.

The system shall be an Internet based remote video visitation system and shall include inmate stations and a limited number of public visiting stations located at LBJ and 4th Avenue Jails controlled via an Operator Control/Reception Station.

The system shall consist of cameras, monitors, microphones/handsets, audio-video switching system, enclosures and all electrical cabling, materials, labor and equipment and services to complete a functioning video visitation system. Proposal responses should provide identified options and future capabilities.

As indicated above, the system will be implemented in multiple phases. Those phases and specific requirements are detailed below.

Contractor shall maintain end-to-end responsibility for VVS, a turnkey inmate Web-based video visitation system, at no cost to Maricopa County. Except for possible wiring needs, Contractor does not require a subcontractor to install or operate VVS. Contractor shall verify the completeness of all components of the system as a routine part of the installation process and continually monitor the system to ensure it operates properly and generates revenues for Maricopa County.

VVS was developed to take advantage of an open architecture that also meets ADA requirements and runs on the Internet. It shall maintain the confidentiality of attorney visitation sessions by blocking them from being recorded or monitored.

Third party and three-way sessions are not permitted. Further, recorded sessions and data can be downloaded to MCSO applications for investigative and statistical purposes and VVS will be

capable of receiving MCSO data, such as to populate inmate accounts, inmate information, balances, etc.

The system, which will be implemented in the requested multiple phases, will consist of all required cameras, monitors, microphones/handsets, audio-video switching system, enclosures and all electrical cabling, and materials needed for ongoing operations. Contractor will ensure that all labor and equipment is needed according to our preliminary implementation schedule.

The system's open architecture allows the terminals to provide more than video visitation. The video visitation terminal can also serve as a kiosk to enable video arraignment and visitation sessions between inmates and their friends or family members, attorneys, and law enforcement officers. In addition to traditional video visitation sessions, it also facilitates the following activities:

- Visitation registration and scheduling
- Inmate information application
- Sick Call application
- Contractor' Secure Instant Mail (electronic mail)
- Commissary order application
- Storage of recorded visitation sessions
- Emergency video application
- Automated retrieval and playback of sessions
- Visitation reporting

Before deploying systems and upgrades Contractor shall perform rigorous quality assurance (QA) testing to ensure minimal to no down time once it is installed. Feature updates shall be provided at no cost to County.

2.2 PHASE 1 -- VIDEO VISITATION/COMMUNICATION KIOSK SYSTEM EQUIPMENT REQUIREMENTS:

Estimated implementation duration: 6 – 9 months

The Video Visitation Solution proposed for the MCSO must meet or exceed the technical requirements outlined in this Section of the RFP. The Hosted Video Visitation Solution proposed to meet these technical requirements must be provided for all MCSO facilities at **no cost** to MCSO including system installation, training, operation and maintenance of the system and its components. It is the intention of the County to utilize the existing kiosk locations in the inmate areas for deployment of the new systems for LBJ and 4th Avenue (when practical). Contractor shall provide County with specific schematics and drawings for the placement of Contractor equipment. County reserves the right of approval for final placement.

The removal of the existing Video Visitation System equipment detailed in Exhibit F shall be the responsibility of the Contractor. The removed equipment shall be delivered to County for disposal.

VISITATION STATION LOCATIONS:

- 2.2.1 Contractor shall perform at no cost to the County, a detailed site survey of the existing electrical systems for all facilities where new and or additional kiosks are required. If the electrical infrastructure is deemed insufficient, Contractor shall be responsible for obtaining all permits and subcontractors to perform the work to County standards. Costs associated with these services are allowable to be included in the ROI calculation detailed in Exhibit "A".
- 2.2.2 County requires that the Contractor provide inmate kiosks at a minimum ratio of 20:1 based on location capacity. A detail of the inmate capacities by location is contained in Exhibit G. The minimum kiosk deployment detail is contained in Exhibit L. If the initial

system has usage of 30% or more of any one station for more than one month an additional station shall be installed at no cost to County. The expansion shall occur within seven days.

- 2.2.3 LOWER BUCKEYE JAIL (LBJ) currently has 144 video visitation stations in place; 48 total inmate visitation stations in the Tower pods; 16 total in the Dorms; 12 in the Psych unit; 6 roll-bouts in the Infirmary; 56 visitors and 6 Legal booths in the visitation lobby. LBJ is to become our central hub for visiting for all inmates in the Durango Triangle (which encompasses Durango Jail, Towers Jail, Tents Jail, Estrella Jail, and LBJ).

The following is an overview of the required minimum number of kiosks to be deployed at this location:

Public Visitor Station: 54 kiosks

Legal Visitation (for attorneys): 8 kiosks

Towers: 96 kiosks

Dorms: 16 kiosks

Psych: 12 kiosks

- in addition to the mounted kiosk 1 roll about port per pod (12 total)

Infirmary: 12 Roll about

Total mounted kiosks: 186

Total mobile kiosks: 12

- 2.2.4 4TH AVENUE JAIL currently has 115 video visitation stations in place; 56 total inmate visitation stations in the Tower pods; 14 roll-bouts in the Special Management Unit (SMU); 38 visitors and 7 Legal booths in the visitation lobby. 4th Ave is to become our central hub for visiting for all inmates in the Downtown Area.

The following is an overview of the required minimum number of kiosks to be deployed at this location:

Public Visitor Station: 38 kiosks

Legal Visitation (for attorneys): 6 kiosks

Houses: 112 kiosks

SMU: 16 roll about

Total mounted kiosks: 156

Total mobile kiosks: 16

- 2.2.5 TENTS JAIL currently has 61 video stations in place; 36 total inmate visitation stations in the Dorm area; 25 total visitor booths. Since we are going to have the central hub at LBJ there is no need to have visitor side locations.

The following is an overview of the required minimum number of kiosks to be deployed at this location:

Public Visitor Station: 0

Legal Visitation (for attorneys): 0

Legal/Medical visitation booths (for inmates): 0

Yards: 29 kiosks

Total Mounted Kiosks: 29

Total Mobile Kiosks: 0

- 2.2.6 DURANGO JAIL currently has no video visitation system in place. Once the new system is installed all visitors will utilize the LBJ Visitor Center or use the web-based application portion to obtain their visits.

The following is an overview of the required minimum number of kiosks to be deployed at this location:

Public Visitor Station: 0
Legal Visitation (for attorneys): 0
Legal/Medical visitation booths (for inmates): 0
Houses: 96 kiosks

Total Mounted Kiosks: 96
Total Mobile Kiosks: 0

Maricopa County may, at its option, choose to decommission this facility, demolish it and build a new facility. In case of this event, it shall be the responsibility of the Contractor conduct the following:

- Remove the installed equipment
- Either place the equipment in storage or redeploy to other locations
- Install equipment in the new facility (if contract time allows)
- Reduce the base usage rate by 1,200 calls per month for the length of time that the facility is unoccupied and or replaced.

- 2.2.7 TOWERS JAIL currently has no video visitation system in place. Once the new system is installed all visitors will utilize the LBJ Visitor Center or use the web based application portion to obtain their visits.

The following is an overview of the required minimum number of kiosks to be deployed at this location:

Public Visitor Station: 0
Legal Visitation (for attorneys): 0
Legal/Medical visitation booths (for inmates): 0
Pods: 48 kiosks

Total Mounted Kiosks: 48
Total Mobile Kiosks: 0

Maricopa County may, at its option, choose to decommission this facility, demolish it and build a new facility. In case of this event, it shall be the responsibility of the Contractor conduct the following:

- Remove the installed equipment
- Either place the equipment in storage or redeploy to other locations
- Install equipment in the new facility (if contract time allows)
- Reduce the base usage rate by 1,200 calls per month for the length of time that the facility is unoccupied and or replaced.

- 2.2.8 ESTRELLA JAIL currently has no video visitation system in place. Once the new system is installed all visitors will utilize the LBJ Visitor Center or use the web based application portion to obtain their visits.

The following is an overview of the required minimum number of kiosks to be deployed at this location:

Public Visitor Station: 0
Legal Visitation (for attorneys): 0
Legal/Medical visitation (for inmates): 3 roll abouts
Pods: 56 kiosks

Total Mounted Kiosks: 56
Total Mobile Kiosks: 3

Maricopa County may, at its option, choose to decommission this facility, demolish it and build a new facility. In case of this event, it shall be the responsibility of the Contractor conduct the following:

- Remove the installed equipment
- Either place the equipment in storage or redeploy to other locations
- Install equipment in the new facility (if contract time allows)
- Reduce the base usage rate by 1,200 calls per month for the length of time that the facility is unoccupied and or replaced.

2.2.9 EQUIPMENT SPECIFICATIONS:

Kiosk Video machines furnished under this contract shall be a hardened steel enclosure to include a touchscreen. The Kiosk Video station must be new or in like-new condition and appearance, in good working condition, and fully operable when installed and during the contract period. The equipment must be approved by MCSO before installation.

The VVS terminal is constructed as a self-contained, hardened steel case that is wall mounted and equipped with a built-in shatterproof touch screen, a high-resolution video camera with integrated lighting, and a handset for audio communication. The steel braided corrections-grade handset can withstand 1,000 pounds of pressure. Surge protection is implemented on each unit with the ability to maintain clean power in the event of a brown-out, where the voltage drops to 6V. The stations come with a custom mounting bracket that ensures a secure, vandalism-proof installation that also prevents hiding of any contraband within or behind the terminal. On the rear of the station the only cables to connect are power and networking: a 3-prong 120-volt (standard PC power cable) and a CAT6 networking cable. The stations do not require additional cabinetry. All equipment will be approved by MCSO before installation.

2.2.9.1 Detention grade hardened steel wall mounted enclosure with rounded top and corners.

2.2.9.2 A shatterproof LCD touchscreen monitor with a minimum of 15" and no larger than 17".

VVS terminals feature shatterproof 15-inch touch screens. Contractor reserves the right to install different terminals or different specifications, as modifications or improvements are realized in manufacturing. Any alternative terminal shall be approved by County prior to deployment.

2.2.9.3 One detention grade audio handset per inmate terminal, and two detention grade audio handsets per visitor terminal, and have portable terminals with handset and speaker option.

Handsets on VVS terminals are detention grade—one on inmate terminals and two on visitor terminal.

2.2.9.4 The terminal will have a built-in camera with built-in LED lighting that automatically activates during video visitation sessions and automatically ends when the video visitation session completes.

VVS terminals have built-in cameras and unique LED lighting to illuminate inmates and those in the visitor center so they can better be seen and also assists in the monitoring and investigative functions.

- 2.2.9.5 The enclosure shall not have any openings exposed to the user. This includes all wiring and ventilation holes.
- 2.2.9.6 The enclosure shall not have any external hinges.
- 2.2.9.7 The terminal must prevent spills from entering the enclosure.
- 2.2.9.8 The terminal must have on-screen signature capabilities to capture an inmate's signature without the use of a "light pen" or other external attachment.

Because VVS terminals are hardened touch screens, they are capable of accepting signatures "written" without having to use a "light pen" or external attachment that could be used as a makeshift weapon within the facility. The system utilizes PINs or other identifiers to determine which inmates are using the system.

- 2.2.9.9 The terminal must be assembled from non-proprietary, off-the-shelf computer components.
- 2.2.9.10 The terminal shall be powered by 110VAC.
- 2.2.9.11 The terminal must have heat syncs and heat vents, located in the back of the terminal, in order to allow for proper cooling.
- 2.2.9.12 The enclosure shall not have a physical on/off switch; it must be able to be remotely shut off by a staff member using a switch located in a secure area.

VVS terminals to not have a physical on/off switch on their exterior. Rather a proprietary magnet is used to activate and de-activate the terminals, preventing inmates from powering them on or off. The software that operates the VVS terminals can be disabled remotely, effectively shutting the terminal off.

- 2.2.9.13 The system must have a LCD "wallboard" viewing officer's station for each facility all located at our central viewing room located at the Lower Buckeye Jail

Authorized County users will be able to initiate, control, record, retrieve and monitor video visitation sessions. One of the primary advantages of implementing VVS is the ability to live monitor and record video visitation sessions. This capability creates new investigative opportunities and also reduces violence within jail walls. In addition, the VVS interface enables jail staff to flag visits for later investigative review and lock recordings from being purged after the standard retention window expires.

VVS sessions can be monitored live by facility administrators by clicking on the "Appointments" icon and then selecting "View." Multiple live sessions can be viewed simultaneously. There are no software-imposed limitations regarding the number of sessions that can be viewed at the same time. Simultaneous sessions will be limited by available bandwidth.

- 2.2.9.14 The "wallboard" station must be a minimum of 60" viewing platform with an array of different configurations for viewing multiple visits simultaneously with

the ability from the viewing station to end visits remotely due to improper conduct.

2.3 WEB-BASED VIDEO VISITATION/COMMUNICATION KIOSK SYSTEM HARDWARE REQUIREMENTS:

- 2.3.1 Digital Recording – The system must include digital recordings of video conversations, in real-time and with historical and playback capability. These recordings can be selectively turned on or off through programming by the vendor, dependent on the type of call and other pertinent legal requests.

Visitation sessions not blocked from recording are automatically recorded and can be played back at any time.

Recorded visitation sessions are downloaded in MPEG-4 format.

Recording of video sessions will be suspended for privileged visitation sessions, such as attorney visits. Attorneys must register in VVS in a custom user group, which will be used as the key to whether a visitation session is recorded or not.

- 2.3.2 Recording Backup – The system shall be equipped with appropriate backup, to reduce interruption of service or data loss.

The video visitation application and data reside on a server that is hosted on Contractor network. This server manages all the interactions between the video visitation terminals and clients and provides secure storage of all data.

All servers located in the Contractor data centers are regularly backed up, and geographically redundant, to ensure the highest quality of service and reduce the potential for service interruption or data loss.

- 2.3.2.1 Legal IP Number Database – The system shall have the capability to allow entries of the name associated with the IP number, law firm, probation, or court and date the IP number was added.

Rather than rely on IP addresses, VVS streamlines this process and reduces database needs because it requires attorneys to register using their Bar ID. Through this process and final verification by facility personnel, attorney visits are kept confidential though a record of the visitation session is still retained.

- 2.3.3 Non-Record Legal Video - Legal Video Visits shall not be recorded.

- 2.3.4 Reproducing Media – Writeable DVD or Blu-ray are the preferred reproducing media to include encrypted password capability.

- 2.3.5 Uninterrupted Power Supply (UPS) – The system shall include a UPS backup for use in the event of a commercial power interruption.

- 2.3.6 Time Synchronized System to a Master Clock – The entire system shall be time synchronized including automatic daylight saving adjustment and Arizona time.

Contractor synchronizes VVS with all time zones to ensure the integrity of time and date data across the system. This synchronization includes adjusting for changes in daylight savings time and Arizona time.

- 2.3.7 Firewall

Contractor will install and maintain firewalls both on site and at our centralized data center in Dallas, TX.

On site, data is both encrypted and authenticated via software algorithms. This occurs at both the inmate video terminal, at on-site friends and family terminals, and at the PC of a home user (during remote visitation sessions).

At our corporate data center, for video traffic from our facilities we utilize a redundant pair of Cisco 5540 Adaptive Security Appliances for the Firewall. For the remote web services, we use an independent, redundant pair of Cisco 5540 Adaptive Security Appliances for the Firewall.

2.3.8 Archival of Records and Recording

2.3.8.1 Contractor shall provide a storage facility for all data.

2.3.8.2 Upon request, Contractor shall furnish the call data records (CDR) and Secure Video Visitation (SVV) records for the previous seven (7) years.

2.3.8.3 Recordings – The Video recordings shall be stored and available online, for a minimum period 2 months, or 60 days.

2.3.8.4 MCSO shall retain access to all data of records and recordings and said access shall survive the termination of this agreement.

2.4 VIDEO VISITATION SYSTEM SOFTWARE REQUIREMENTS:

2.4.1 The video visitation scheduling, user management, and policy management, must be web-based and allow for MCSO to administer visitation sessions and visitation operations based on MCSO policies

VVS makes the complex tasks of scheduling sessions and managing user accounts easy and secure for the facility, friends and family members, and inmates. The following highlights many of the features and functions inherent in VVS.

User Account Set-up and Scheduling for Friends and Family Members

- Web-based and accessible from any standard Web browser
- Simple user interface, enabling account set-up and scheduling to be completed in minutes
- Automatically support multiple facilities in multiple locations with multiple housing units, making it easy to “find” the desired inmate
- Automatically displays only the visitation times and dates that are available
- Automatically sends an email confirmation when a visit is scheduled, modified, or cancelled
- Allows users to easily change their personal information (password, address, phone number, etc.)

User Account Control and Scheduling Features for the Facility

- Secure, Web-based access anytime/anywhere – providing different levels of authority and requiring unique user names and passwords
- Point and click to view thorough user information including photo ID and easily approve or reject a user account
- View, manage, report, and modify scheduled visits from the VVS dashboard
- Review historical staff usage through system user logs

Scheduling Features for Inmates

- Terminals with simple touch screens and user-friendly, basic icons - providing inmate access in English, Spanish, and any other language requested by Maricopa County
- Large letters and numbers that clearly display pending visits
- Built in lighting to enhance screen images

- On-screen timer to show remaining time throughout the entire visitation session

2.4.1.1 Legal Visits (Private Attorneys) – Legal Visits are considered right to counsel confidential. These videos are not recorded or monitored and may be charged for Web usage.

While attorney calls are private and not recorded, they still are logged and charged so that Maricopa County can earn commission payments on them and track the activity. Records of all visits that have occurred are stored even though the visit is not recorded. This valuable information shows that attorneys have had access to their clients. Records are stored for three years.

2.4.1.2 Legal Visits (County Public Defenders/Prosecutors)-Legal Visits are considered right to counsel of confidential. These videos are not recorded or monitored and will not be charged Web usage.

While attorney calls are private and not recorded, they still are logged and charged and Maricopa County can earn commission payments on them. There is a record of all visits that have occurred. This valuable information shows that attorneys have had access to their clients. Records are stored for three years.

2.4.1.3 Free County Agency Visits (i.e. Adult Probation, Sheriff's Deputies, and Officers of the Court) – These videos are not considered right to counsel confidential. The Video is recorded and monitored and is free from Web usage.

Contractor records all visitation sessions that are not private and privileged. Contractor will work with Maricopa County to establish custom user groups that identify sessions for which there will be no charge to users.

2.5 SYSTEM FEATURE REQUIREMENTS:

Contractor' technology is flexible and does not mandate rigid specifications when working with facility-owned systems, JMS, OMS, commissary, vendors, etc. Contractor will fully cooperate with your facilities and vendors to automate the systems.

The most common technologies Contractor uses to integrate with your systems include: SOAP Web Services, HTTP, FTP push or pull of files in any textual format, JSON, XML-RPC, and TCP Sockets. All of these methods are performed over a secure connection.

Contractor is able to transform your data format for insertion into our platform, negating the need for costly code modifications to your system. Contractor integration engineers will consult with your facilities' IT department or system provider to determine the best integration strategy for your specific application.

The dedicated Contractor Integration team designs, develops, tests, and implements all custom integrations with corrections industry and banking systems. Our mission is to deliver fast and flexible solutions for our customers. This process is incorporated into the overall Project Plan, included as Appendix A, for the installation of the Contractor SCP inmate telephone system. Major milestones include:

- Collect Preliminary Needs/Requirements
- Contract Signed
- Finalized Requirements document
- Approved Scope Statement
- Finalize Design Document
- Schedule Customer Implementation
- Develop Custom Integration Solution
- Test Custom Integration Solution
- Implement Custom Integration Solution

- Customer Approval and Sign-off

2.5.1 Inmate Personal Identifier (PIN) – The system shall provide unique Personal Identification number to each inmate and user. The system shall interface with MCSO's Jail Management System (JMS). Inmates shall establish a PIN number upon first use of kiosk system.

2.5.2 Multi-lingual inmate interface (English and Spanish at a minimum).

2.5.3 A single system must be able to support multiple facilities in multiple locations with multiple housing units.

2.5.4 Web-based visitation scheduling for authorized users (MCSO Services staff, attorneys, the public) utilizing any standard web browser.

Inmates' friends and family members access a simple Web site via the Internet, designed with the look and feel of other Contractor systems. The inmate's friend or family member schedules and pays for a video-visitation session by going to www.securustech.net Web site.

Using the video visitation Web site, they can select the facility and inmate they wish to participate in the video visitation session. The scheduling application automatically schedules visits according to the inmate's dormitory, which terminals are available at that location, and available session times for video visitations to be held. Fees are accessed and collected at the time the visit is scheduled via credit or debit card.

VVS receives inmate information, including housing location, from the JMS. Our system then dynamically identifies whether the inmate is located in an area with a video visitation terminal, whether a terminal is available based on date/time of the requested visit, and automatically displays only available times to the person scheduling the session.

VVS allows user fees to be assessed for remote or at-home visitation sessions and collected by the system. As friends and family or members of the public elect to conduct remote visitation sessions, they pay for the session on a per-session charge.

2.5.5 Inmate terminal must display pending visits and scheduled medical appointments.

The system shall only show a session is scheduled and does not define the kind of session, such as a medical appointment, providing privacy for inmates and conformance with HIPAA requirements.

2.5.6 Web-based scheduling system must allow users to easily and simply schedule a visitation session.

2.5.7 Web-based scheduling system must require visitors to provide valid photo ID in accordance with MCSO Policy DK-3, Inmate Visitation before signing up for a visitation session

Friends and family members are required to provide proof of identity when registering for VVS. Failure to do so nullifies their enrollment and prevents them from being able to schedule visitation sessions. Friends and family members' identities can be easily verified by authorized Maricopa County users.

2.5.8 Web-based scheduling system must only display timeslots that are available for each individual inmate in conjunction with JMS and other scheduled Inmate functions included but not limited to future court dates, medical appointments, and programs.

VVS displays only available time slots to friends and family members to avoid double-booking appointments. Inmates can easily see appointments scheduled for that day by pressing the Appointments icon on an VVS terminal. To track inmates, VVS interfaces with the JMS and takes data feeds approximately every 15 minutes. If an inmate is moved to court or the infirmary, for example, any sessions scheduled for that inmate during that time period will be automatically cancelled and notification sent to the individual who scheduled the session.

- 2.5.9 Web-based scheduling system must conduct all conflict checking and only display times that are available.
- 2.5.10 Web-based scheduling system must allow users to easily change their personal information (password, address, phone number, etc.).
- 2.5.11 Web-based scheduling system must send an email to the visitor when a visit is scheduled, modified, or cancelled.
- 2.5.12 If a scheduled visit is cancelled, the timeslot should become available for scheduling.
- 2.5.13 Web-based scheduling system must assign a unique visitation identification number for every visit for reporting and tracking.
- 2.5.14 System must use set durations of 20 minute increments for each on-site visit, or in increments to be determined by MCSO Command Staff.
- 2.5.15 System duration for online Web to be determined by County.
- 2.5.16 Security Levels for Users - The system shall be capable of assigned password access for different levels of security to include System Manager, System Administrator, User Security Level Access by task and location.
 - 2.5.16.1 Each user will require a unique username and password that will dictate their level of functionality.
 - 2.5.16.2 The system provides authorized users the ability to do searches and create reports.
- 2.5.17 Video Searching – The system shall be capable of searching records by Booking number, Inmate name, Visitor name or assigned number, IP address, Visitor ID number, and date/time.
- 2.5.18 The system shall detect when extra people or voices are present and a notation shall be included in the video detail record of the attempt.

Contractor's VVS does not currently have the ability to detect extra people or voices during the Video Visitation Session.
- 2.5.19 Attachment of Notes to Video Records – The system shall have the capability of attaching up to six (6) notes of at least 50 characters to any call record to include information such as case number or other investigative data.

Though this feature is not directly available in our VVS product, the ability to attach notes to VVS session recordings can be accomplished using our proposed THREADS™ investigative tool. Contractor is experienced in developing such applications and has developed this feature, which is currently available to users of our inmate telephone system. We are currently in the process of developing and exploring such capabilities in products such as VVS; we continue to develop capabilities for VVS that mirror the

capabilities in its inmate telephone system. This ensures continuity of use between SCP and VVS.

- 2.5.20 The system shall provide a visual countdown clock to inform visitor of how much time s left.
- 2.5.21 The system shall provide a visual warning message to inform the visitor that the visit will be ending in 2 minutes.
- 2.5.22 The system shall automatically cancel any pending visits if inmate is in-process or has been released from jail.
- 2.5.23 The system provides a way to display scheduled visits to Staff so they know where and when an inmate needs to be available for pending video visits.
- 2.5.24 Authorized personnel must be able to quickly and easily schedule visitation sessions.
- 2.5.25 The scheduling and management system must be able to communicate with the video hardware at the time of a scheduled visit so that the visitation session will automatically commence without staff involvement.
- 2.5.26 The video visitation system must have visitation recording capabilities.
- 2.5.27 The kiosk must be able to access the web-based application and be enabled for touch screen inputs.
- 2.5.28 The kiosk will provide the inmate with standard information that is retrieved from the facility's jail management system. Standard information would include such things as upcoming court dates, Inmate account balances, and visits.
- 2.5.29 Provides an audit trail of all system activity (i.e., user login times and locations, which users have scheduled/modified/cancelled a visit, etc.).

2.6 SUBSEQUENT PHASE PLANNING

For the phases detailed below, Contractor shall consult with County and develop a detailed implementation plan for each phase. The order and approximate length of each phase may be changed by County at any time with notice to Contractor. If Contractor fails to meet any timelines agreed to between the Parties, Contractor may be deemed to be in default and corrective action may be deemed necessary (up to and including termination, or modified revenue sharing rates).

2.7 PHASE 2 – INMATE RULES AND REGULATIONS REQUIREMENTS

Estimated implementation duration: at start-up

- 2.7.1 The complete *Rules and Regulations for Inmates* will be available electronically on the kiosk. Inmates will be required to acknowledge the availability of these rules and regulations with an electronic signature when they establish their Personal Identification Number.

Currently under development, VVS will be capable of enabling inmates to read documents such as MCSO's Rules and Regulations on the terminal. Inmates will be required to access the documents using unique PINs, which will be used to verify and acknowledge that they have read any required documents.

- 2.7.2 If an inmate who is still in custody after 48 hours from the time they are accepted into custody and they have not yet acknowledged the availability of the Rules and Regulations for Inmates on the kiosk, an electronic message will be forwarded to the commander of the Bureau Hearing Unit, or his designee, for appropriate follow-up.

Contractor is considering this capability but has not yet scheduled it for our development road map. As a functional equivalent and until it is firmly identified as an enhancement to VVS, Contractor system administrators will generate compliance reports required by Maricopa County to provide this capability without additional work for the County.

2.8 PHASE 3 – INMATE FORMS REQUIREMENTS –INMATE REQUEST FORMS & LEGAL REQUESTS

Estimated implementation duration: 1 month

2.8.1 The inmate will complete Inmate Request Forms and legal requests via touch screen keyboard and be signed for by using signature screen without using a light-pen or other attachment.

2.8.1.1 The forms shall be automatically routed to the appropriate locations where they can be processed.

VVS is currently configured to route forms to a queue that can be accessed based on one of three groups authorized users are granted security permissions to. Contractor is willing to work with Maricopa County to better understand your needs in this area and develop such routing capabilities.

2.9 PHASE 4 – INMATE CANTEEN REQUIREMENTS

Estimated implementation duration: 1 month

2.9.1 The kiosk will provide for commissary ordering with real-time account balance via touch screen inputs.

Contractor will interface VVS with Maricopa County's commissary ordering system to display account balances that will be updated based on the refresh cycle established between the two systems. Real-time updates can be made though they would have to be initiated from the commissary system.

2.9.1.1 Commissary application shall have pictures of products.

2.9.1.2 Commissary application shall reasonably replicate the functionality of the County's current commissary systems.

2.10 PHASE 5 – INMATE FORMS REQUIREMENTS – GRIEVANCES AND APPEALS

Estimated implementation duration: 1 month

2.10.1 The inmate will complete grievance and appeal forms via touch screen keyboard and be signed for by using signature screen without using a light-pen or other attachment.

VVS's Grievance Module is a two-way communication vehicle between inmates and the facility and will be acknowledged by the inmate by either accepting or rejecting the facility's grievance response.

2.10.1.1 The forms shall be automatically routed to the appropriate locations where they can be processed.

2.11 PHASE 6 – INMATE E-MAIL REQUIREMENTS

Estimated implementation duration: 1 month

2.11.1 The kiosk will provide an Inmate Email solution.

- 2.11.1.1 Inmates will be able to receive an email from an approved user that pays and prepays for response. Emails shall be no more than 500 characters in length.
- 2.11.1.2 The email system shall have a word recognition program that can identify certain words, phrases, or slang and flag it.

2.12 PHASE 7 – CORRECTIONAL HEALTH SERVICES REQUIREMENTS – HEALTH CARE NEEDS FORMS

Estimated implementation duration: 1 month

- 2.12.1 The inmate will complete Health Care Needs Requests via touch screen keyboard and be signed for by using signature screen without using a light-pen or other attachment. The County understands that said functionality is not available as of the execution of this contract and that Contractor shall make all reasonable efforts to meet this requirement in the future.

- 2.12.1.1 The forms shall be automatically routed to the appropriate locations where they can be processed.

- 2.12.2 The kiosk will provide for sick call reporting via touch screen inputs.

2.13 FUTURE DOCUMENTS AND APPLICATIONS

- 2.12.1 The system will include the capability to add additional document applications and/or upgrade previously installed documents and applications as necessary.

3.0 INTERFACE REQUIREMENTS

The proposed system must interface with MCSO data systems using MCSO-preferred transaction-oriented protocols in near real-time within our secure network environment. The preferred approach is via a vendor centralized server connection to the County Integration Engine to minimize external connectivity to the MCSO network. The County Integration Engine is used to facilitate connectivity between systems using a myriad of transport and data formatting protocols. The County Integration Engine uses IBM WebSphere MQ messaging as the preferred transport for guaranteed store-and-forward delivery. In this configuration, the County's MQ messaging server would host connections to the vendor system, which would run MQ client software.

Additionally, MCSO maintains a full, parallel development/test environment for IT systems. Vendor systems should integrate with existing MCSO systems and processes and should support a full development/test environment. Please elaborate on how your proposal will meet or exceed these requirements.

For the initial implementation of the web-based video visitation system (WVVS) a small set of transactions should be implemented to help coordinate the scheduling of inmates for visits. The Jail Management System (JMS) holds the schedule for all inmates' time commitments. System integration transactions between the WVVS and the JMS should be created to help coordinate the scheduling of inmate video visits. As an example, there should be a transaction sent by the WVVS to the JMS requesting a list of scheduled appointments for a given time period (one day or more). With the JMS response the WVVS would be able to determine and display available time slots for visitation.

The most common technologies Contractor uses to integrate with your systems include: SOAP Web Services, HTTP, FTP push or pull of files in any textual format, JSON, XML-RPC, and TCP Sockets. All of these methods are performed over a secure connection.

Contractor is able to transform your data format for insertion into our platform, negating the need for costly code modifications to your system. Contractor integration engineers will consult with your facilities IT department or system provider to determine the best integration strategy for your specific application.

Contractor Integration Process

The dedicated Contractor Integration team is our dedicated group of individuals that designs, develops, tests, and implements all custom integrations with corrections industry and banking systems. Our mission is to deliver fast and flexible solutions for our customers. This process is incorporated into the overall Project Plan for the installation of the Contractor SCP inmate telephone system. Major milestones include:

- Collect Preliminary Needs/Requirements
- Contract Signed
- Finalized Requirements document
- Approved Scope Statement
- Finalize Design Document
- Schedule Customer Implementation
- Develop Custom Integration Solution
- Test Custom Integration Solution
- Implement Custom Integration Solution
- Customer Approval and Sign off

Development/Testing

Contractor will integrate with existing MCSO systems and processes and to support a full development/test environment. Contractor supports and utilizes today a four level IT environment today:

- Development
- Quality Assurance
- Pre-Production
- Production

Scheduling of Inmates' Time Commitments

VVS schedules based on information from its most-recent JMS data feed. When an inmate is registered in JMS as being unavailable for whatever reason, any video visitation sessions for that inmate in that time period are automatically cancelled by the system. For example, if a video visitation session is scheduled for an inmate at 10 a.m. on a Monday morning but the inmate is moved to the infirmary at 9 a.m., when VVS receives that data it will automatically cancel that session and issue a credit for the session to the visitor, who can reschedule at their convenience.

4.0 NETWORK:

- 4.1 Active network and associated equipment shall be owned and maintained by MCSO. This equipment and interconnections shall be purchased by the vendor, as per our specifications, as part of the "no cost" initiative. The active network equipment will be composed of Cisco router and switch devices, which will be interconnected site-to-site via Metropolitan Optical Ethernet circuits. These network devices shall be configured for use by the vendor to insure proper compatibility with their end devices.

Because of the high bandwidth demands for the VVS system's network requirements, Contractor proposes to operate the system on a separate, parallel network that will offer equivalent or higher levels of service than from piggy-backing on MCSO's network. While MCSO will own the network that Contractor procures and installs, operating it separately will maximize efficiencies of both networks because of the resource demands of transmitting audio and video signals. Contractor will configure and install network devices are both compatible with end devices and will optimize network functionality.

- 4.1.1 The video visitation system shall be a complete IP-based system. All video and audio streams between the terminals, visitors, and management equipment (servers) shall be transmitted over Ethernet.

- 4.1.2 Systems that utilize analog audio/video matrix switching systems are not acceptable.

VVS is fully Web based and digital, and does not have analog components. It is a centralized system that allows automatic technology and feature upgrades. After the video visitation system has been implemented, it is easy for Contractor to enable new features and modules by activating the feature in the centralized system.

- 4.1.3 The video visitation solution shall consist of inmate kiosks connected over a 1Gbps local, dedicated Ethernet network. Each site shall be connected to other sites via a 50Mbps CenturyLink Metropolitan Optical Ethernet circuit. These MOE circuits shall reside in a private cloud through CenturyLink.

Contractor will provision and implement the network VVS operates on and ensure that it includes sufficient bandwidth to meet the visitation needs of Maricopa County, your inmates and their friends and families. Contractor will upgrade the network and VVS as necessary during the life of the agreement.

- 4.1.4 The visitor terminal shall be able to access the video visitation solution via local area network (LAN) and via a broadband internet connection (DSL, cable, etc.) using a computer or laptop that is web camera and headset enabled.

- 4.1.5 High quality video using low bandwidth

- 4.1.6 Video Standards: H.264

- 4.1.7 Video Transmission Speeds: 64 Kbps – 2 Mbps

- 4.1.8 Wide range of video resolutions and bit rates: CIF (352 x 288 pixels), SIF (352 x 240 pixels), QCIF (176 x 144 pixels)

- 4.1.9 Constant or variable bit rate and frame rate

- 4.1.10 Must provide encryption for all visits

4.2 CABLE/ELECTRICAL POWER:

- 4.2.1 The Contractor shall be responsible for the installation of all necessary low voltage CAT6 cable, power lines, electrical hookups, for each video kiosk with control in each facility.

- 4.2.2 Existing house cable used to provide services becomes the property of MCSO.

Contractor will replace all existing cable on Maricopa County's current video visitation systems with new CAT6 cable.

- 4.2.3 Power, Grounding and Cooling Requirements

VVS terminals have the following environmental requirements:

- Operating temperature range: -4°F to 122°F (-20°C to 50°C)
- Power: 110V, 2.5 amps
- Grounding: All terminals require a three-prong grounded power outlet
- BTU: Each terminal generates approximately 210 BTUs during a visitation session with the lights operating.

4.3 INVESTIGATIVE TOOLS/INTELLIGENCE GATHERING:

The system shall have the ability to provide investigative tools, features, and creative solutions that would enhance MCSO's capability to actively monitor and data mine criminal activity being conducted by inmates in the jails through the Web-Based Video Visitation/Communication Kiosk System.

Contractor shall provide Maricopa County with our new, powerful investigative software called THREADS™, exclusive to Contractor and not available from any other provider. THREADS will enable Maricopa County investigators mine intelligence data like never before and uncover criminal associations quicker and more efficiently, such as interfacing with TouchPay kiosks to follow the money trail of who made deposits or paid for video sessions and associating that information with other investigative data.

Contractor understands the lifecycle of intelligence and investigating communications data and the challenges investigators, detectives, and corrections facility staff face in both time and resources, such as the following:

- Pulling reports
- Exporting information
- Sending information to someone else
- Contacting other facilities for information
- Combining all the information together
- Receiving information in many different formats
- The daunting task of identifying suspicious behavior in the information provided to uncover focused leads

The Contractor THREADS product provides the means to answer these questions. The unique algorithms used within THREADS were designed by real investigators with many years of experience analyzing communications data and training other investigative units on how to analyze data.

Managing Investigative Data

Sources of Information

Corrections Data	External Data
<ul style="list-style-type: none"> • Inmate call records • Inmate personal information (such as name, account number, PIN, DOB, and SSN) • Who the inmate is allowed to call versus who is actually called • Called party billing name and address information • Public phone records 	<ul style="list-style-type: none"> • Confiscated cell phones (such as calls, text messages, emails, videos, and contacts) • Corrections facility information in proximity to calling behaviors • Events and places of interest • Mail • Lexus Nexus • SS7 information

All corrections data (such as call records, phone numbers, billing name and address) is automatically and fully integrated with THREADS the moment THREADS is enabled. All other sources of data are imported into THREADS and analyzed together to automatically build an investigation.

After determining a suspect on the outside of the facility is involved and mapping out the address, the investigator acquires the public phone records and imports that information into THREADS, which is again analyzed with all the other gathered information. This all takes place in one location, with one tool, and is completely integrated with inmate data.

Powerful, Accurate, Easy to Use

THREADS is a powerful, accurate, easy-to-use, intuitive tool that will automatically analyze investigative data such as inmate communication records, public phone records, and data from confiscated cell phones to automatically generate focused leads for investigators. Leads can

include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple inmates, their correlation to called parties, and much more.

Additionally, this powerful software provides dayroom-based analysis that discovers leads irrespective of the PIN being used by the inmate and common contact reporting showing inmates who are facilitating communications between different areas of the institution. Maricopa County investigative staff can easily uncover patterns of fraternization between inmates and correctional officers, discover common contacts between inmates and called parties, and customize the information and reporting to filter out irrelevant calls such as to girlfriends or legal counsel from analysis.

THREADS will detect criminal organizations being run from within jail, detect three-way calling patterns when multiple inmates are talking to one called party at the same time, find associations of multiple called parties based on who is calling them, and identify inmates who possibly have a cell phone based on calling patterns. For instance, if an inmate makes six calls per day, every day, but then all of a sudden doesn't make any for a week, it is possible they have another way to communicate, such as a cell phone.

Graphic Representation

All information is presented graphically as well as textually such as the example presented in the following figure.

Timeline charts and graphical analysis make it easy to show periods of high-intensity calling and other calling patterns on a graphical and interactive timeline. This technology identifies the inmate even if the calls are masked by another inmate's PIN and eliminates the human intervention by receiving actionable intelligence at the push of a button. Additionally, THREADS allows you to set up automated notifications, which will email an investigator when information is found.

THREADS analyzes data for investigators and provides interactive visualization tools to produce easy-to-understand analytical reports, charts, interactive graphs, maps, and builds a case and presentation view that can be used as evidence in a criminal trial.

Investigative Benefits for Maricopa County

- Cell phone forensics analysis
- Identify accomplices
- Inmates contact people on the outside indirectly, identify who they are "really" contacting
- Identify linkages
- Identify an inmate's inner circle
- Identify associated gang members
- Identify an inmate's communications within jail
- Find unique patterns in communications data
- Combine all the data into a single system to analyze
- Harvest all of this information with enhanced reporting tools

Contractor' THREADS is an exclusive investigative technology that no other provider can offer to the correctional industry. THREADS will be available as an optional product and empowers Maricopa County with the latest in investigative technology and one of the most powerful investigative tools in the intelligence community.

4.3.1 Random Monitoring of Live Video in Progress – The system shall provide the ability of randomly monitoring live Video and record and review with a rewind function.

Contractor Video Visitation allows real time viewing (monitoring) of video sessions and interrupt from a computer (smart phone and tablet coming soon) for authorized users. Live viewing can be done at the facility or remotely. Authorized users can view live sessions with a standard computer and a broadband internet connection.

The system has the capacity to simultaneously record the visitation sessions from all installed stations.

Contractor Video Visitation allows the facility to record sessions either predetermined by user profile, for example all offenders, or ad-hoc, for example where suspicious behavior is seen. All recorded sessions are stored in an encrypted file format and only users with proper permissions can view recordings. Recordings are hosted in through the centralized network. All recordings are logged and time-stamped for traceability and to ensure integrity of the recordings. Contractor anticipates enhancements to the recording functionality, which will include additional search capabilities, download capabilities, and recording user management capabilities.

Depending on the facility's data retention policy, Contractor can set the recorder software to have 30, 60, or 90-plus day retention cycles. Transferring recordings to mobile media is available, and Contractor can provide recordings on request. Administrator access to transfer recordings is currently under development.

THREADS™

A Contractor exclusive, lead generating, analytic technology and is not available from any other provider. THREADS is a powerful, accurate, and extremely easy to use software application that will automatically generate leads for investigators by uncovering calling patterns, associations between multiple offenders, and their correlation to called parties.

THREADS will automatically analyze investigative data such as offender communication records, public phone records, and data from confiscated cell phones to generate focused leads for investigators. Leads can include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple offenders, their correlation to called parties, and much more.

- 4.3.2 Ability to Automatically Notify an Investigator – The system shall provide the ability to remotely notify an investigator when a targeted inmate is visiting or has visited or an IP address is being used or has been used.

This function is currently on the VVS road map and targeted for development at a later time.

- 4.3.3 Transcribing Email (English and Spanish) Search – Ability to translate multiple languages from Inmate Email.

Contractor inmate email application, Secure Instant Mail (SIM) is the application we propose for inmate email. SIM has the capability to translate between Spanish and English and English to Spanish.

4.4 INSTALLATION REQUIREMENTS:

- 4.4.1 All costs Associated – The contractor shall be responsible for all costs associated with the Web-based Video Visitation/Communication Kiosk System, including purchase, installation, service, maintenance and operation. The Sheriff's Office shall have no responsibility for any costs associated with the installation or on-going maintenance of the system, excluding the network.

- 4.4.2 Space Requirements

VVS requires the following space, environmental, and electrical power requirements:

- Space: Outside dimensions of VVS terminals are 21" x 17" x 6" (H x W x D). The video visitation application and data reside on a server that is hosted on Contractor' network. This server manages all the interactions between the video visitation terminals and clients and provides secure storage of all data.

- Environmental: VVS units are designed for a typical correctional environment and do not require any special environmental conditions.
- Electrical: VVS units use a three-prong 120-volt (standard PC) power cable.

4.4.3 Implementation Plan (Attachment J)

4.4.4 Coordinating Removal of the Current Video Visitation Systems – MCSO currently owns the Inmate Video Visitation System in place at 4th Ave Jail, Lower Buckeye Jail, and Tents Jail. When a new contractor is selected as a result of this RFP, a coordination team shall be formed for a smooth and orderly transition from the current system to the new system. This team will consist of MCSO personnel, FMD and the new contractor. This transition should cause minimum service interruptions. A new contractor may install new cable or acquire legal rights to the existing cable. Minimal disruption of service is required for new installation.

4.4.5 System Testing

4.4.5.1 The Contractor must describe, in its response, how it performs standard system testing to ensure that the proposed Web-based Video Visitation/Communication System and its network services are fully implemented and ready to accept visitation traffic and MCSO use. This description must include the Contractor and industry standard methodologies, procedures and protocols consistent with the Web-based Video Visitation/Communication Kiosk System proposed for MCSO.

After each facility is transitioned, our Project Manager and Field Service Technician will review our quality checklists with the Maricopa County Team.

Weekly stakeholder meetings will be hosted by the Contractor Project Team and will involve participation from the Maricopa County Team.

At the beginning of the implementation project, the Contractor Project Management Team will work with the Maricopa County Team to identify key stakeholders, primary points of contacts, and roles/responsibilities for the duration of the project.

The Contractor Project Management Team will establish regular meeting forums and communication protocols that accommodate the requirements of the Maricopa County Team.

Throughout the duration of the project, our Project Management Team will provide weekly installation progress reports. The reports will include updates on all active, completed, and pending installation activities.

In addition to the personal communication from our Project Managers, Contractor can set-up automated email notifications for the Maricopa County Team. The automated email notifications are a great way for our customers to receive updates on status changes for major milestones and other tasks of interests.

4.4.5.2 The Contractor must describe what is required of MCSO personnel during this system testing. All hardware, software, software licensing, etc. required to perform this testing must be provided to MCSO at no cost.

Contractor' demand on MCSO personnel's time is minimal, requiring only the following:

- Escorts in appropriate areas for security purposes

- Project management resources and time to finalize and approve installation plans
- Project management resources and time approve work at key milestones
- Project management resources and time for final approval of system installation
- Project management resources and time for status meetings at regular intervals during installation

Contractor will provide all hardware, software, software licensing, etc. to MCSO at no cost.

4.4.5.3 The Contractor is required to provide system testing which simulates normal operating conditions of the installed Hosted Video Visitation Solution to ensure proper performance after hardware and software configuration is complete. This simulation must include full traffic load representing high traffic situations for visitation traffic.

4.4.5.4 The Contractor must agree, in its response, to MCSO's right to require the replacement of any network service or system component whose failure to meet required performance levels during testing has risen to chronic problem level.

Contractor will replace any network service or system component whose failure to meet required performance levels during testing has risen to chronic problem level.

4.4.5.5 Contractor - After cutover of any portion of the system, the contractor shall conduct acceptance tests consistent with factory system performance specifications.

4.4.5.6 MCSO - The Sheriff's Office shall also complete a test regimen based upon features and performance as specified in the contract.

4.4.5.7 Action Item List – An action item list will be developed for any issues resulting from the testing. A mutually agreed upon time table will be developed and implemented for all action items to be resolved.

4.5 MAINTENANCE, SERVICE AND SUPPORT:

4.5.1 The contractor must submit a detailed explanation of the maintenance and repair plan. If the problem involved is an equipment failure, MCSO shall be provided a root cause analysis report within thirty (30) days of the incident.

Contractor VVS is centrally monitored and managed through the most comprehensive maintenance and repair network in the corrections industry. Monitoring begins with our state-of-the-art Network Operations Center (NOC), extends to our Technical Support Center, and on-site maintenance will be handled by the on-site administrators assigned to MCSO supplemented by field services technicians strategically located to provide any additional support needed.

VVS is constantly monitored by Contractor employees from our NOC at our headquarters location in the metropolitan Dallas, Texas, area. This service center is staffed 24x7x365 by network experts who are certified in the systems and software used to monitor all SCP functions and equipment, as well as the associated network. The NOC maintains failure reports, service history, and other diagnostic information, which will be available to the County when requested.

The NOC will maintain the names and contact information for each Contractor employee supporting Maricopa County. They will be accountable for any actions required to

prevent or repair any outages. Contractor will follow the County's protocols for communicating outages or repair actions in the unlikely event these occur.

Contractor Network Operations Center in Dallas, TX

Premium Network Monitoring Capabilities

Contractor proactively identifies potential system and network abnormalities through a centralized diagnostic application, Orion by Solar Winds. This network management software allows Contractor personnel to continuously monitor all hardware, software, and system metrics.

Through our network monitoring practices, we are able to complete the following functions:

- **Enable proactive repairs to a system to prevent it from going down.** Many times corrections are made before a system shows signs of an issue and before the facility is aware of a problem. This means less down time and increased system reliability for the facility.
- **Alert remote or on-site engineers of any system threshold inconsistencies or alarms.** If detected:
 - Alerts are sent to the NOC to track the event.
 - The NOC communicates with engineers through email, short message service (SMS), or directly through a wireless phone to address the issue.
- **Receive real time alerts when the system detects an error.**
 - Identifies if the network elements health threshold has been exceeded or if any other potential system issue has been discovered.
 - Establishes volume thresholds for each transport carrier on core node equipment at each data center, alerting Contractor personnel of possible carrier network issues.
- **Monitor call traffic patterns, bandwidth detail, and network life cycle management to ensure sufficient resources are in place.** A separate capacity engineering team reviews call traffic volume reports and storage requirements throughout all systems.
- **Centrally monitor all calling traffic and reporting to determine if increase or decreases in the number of telephones are needed.** Upon agreement by the County, the service and operations team will install any additional telephones required.

Remote Programming, Diagnostics, and Troubleshooting

The Contractor NOC uses the Orion network monitoring application to constantly check the system to ensure optimum performance and to anticipate the need for additional network or capacity.

Visual monitoring in our NOC is achieved through the use of several key screens that are constantly updated and monitored by our personnel in our NOC.

The NOC can contact the Technical Support Center (TSC) if it determines that another level of technical support may be needed to address issues or concerns. This action could involve dispatching a Field Services Technician to a Maricopa County facility.

Technical Service Center

The Contractor Technical Services Center (TSC) uses a call distribution system to automatically manage the flow of inbound customer calls. The TSC provides a single-point-of-contact where a facility may inquire on items such as remedial maintenance issue or trouble that may arise 24x7x365. Clients can contact the TSC by any of the following convenient methods to obtain service:

- **Telephone** – 866-558-2323
- **E-Mail** – technicalsupport@securustech.net
- **Fax** – 800-368-3168
- **Web portal** - <http://www.securustech.net/facility/Default.asp>

The technical service center offers the following features to our clients:

- Technical support and field dispatch 24x7x365
- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure Service Level Agreements are met
- Certified technicians to provide quick problem resolution
- Ownership of every issue via training, support, other departments, and historical information
- System and individual site connectivity monitored 24x7x365

24x7x365 Contractor Technical Support Center

Contractor technicians receive internal Contractor certifications, based on our business and the products and services we support.

Service Levels

When a facility calls Contractor, the event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a resolution timeline and escalation procedure. In all cases, Technical Support will respond in the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when a system event adversely affects the operations in multiple housing units.

Response time for a P1 event is two hours. If a dispatch is not required, Contractor notifies the facility when the service issue is resolved; if a dispatch is required, Contractor contacts the customer and provides an estimated time of arrival.

A P1 event is escalated to the following groups and persons:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If resolution is delayed, escalation procedures within the Contractor Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Priority 2 Service Level

A Priority 2 (P2) assignment occurs when a system event adversely affects system functionality in an entire housing unit.

Response time for a P2 event is 24 hours. If a dispatch is not required, Contractor notifies the facility when the service issue is resolved; if a dispatch is required,

Contractor contacts the customer and provides and estimated time of arrival. A P2 event is escalated to the Technical Support Department.

Priority 3 Service Level

A Priority 3 (P3) assignment occurs when a system event adversely affects a single terminal or multiple terminals.

Response time for a P3 event is 72 hours. If a dispatch is not required, Contractor notifies the facility when the service issue is resolved; if a dispatch is required, Contractor contacts the customer and provides and estimated time of arrival. A P3 event is escalated to the Technical Support Department.

Escalations

If a dispatch is not required, Contractor notifies the facility when the service issue is resolved. If a technician is required, Contractor contacts the customer with an estimated time of arrival.

The following supervisory personnel represent the escalation chain:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- VP Service and Technical Operations

Centralized Services Operations Model

All Contractor' services and operations are managed centrally, from our Services and Operations organization in the metro-Dallas, Texas area. The Operations team is responsible for supporting external customers; this includes Customer Service, Field Services, Installation and Engineering, and Technical Support. The Support Services team is responsible for providing internal support services; this includes Quality, Training and Customer Satisfaction, and Reporting and Analysis.

Service Ticket Routing

The TSC manages the flow of inbound calls through a call distribution system that routes calls directly to our support technicians in a skills-based, platform specific manner. Contractor establishes response times and service level agreements that accomplish our key objective of providing timely resolution to each request. Service calls are answered 24x7x365 by live technicians to provide timely and quality customer service.

Field Service Technicians (FSTs) will be routed to all service requests through the Contractor trouble ticketing process.

In all instances, service will be requested through the TSC and service personnel will be dispatched through trouble ticketing system to ensure documentation and timely resolution of all service tickets.

Event Tracking System

The Contractor event tracking system logs, tracks, manages, and assures appropriate response to all service requests. The service request generates a unique trouble ticket number that is linked to each facility's service history and provides real-time updates. Each ticket has a priority level assignment, which drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem, and resolves the problem or engages the appropriate party for problem resolution.

The TSC maintains ownership of all service requests and is responsible for the escalation and update functions. Every effort is made to resolve problems remotely and within the framework of resolution timeframes. However, if the problem requires on-site service, a technician will be dispatched to the facility to expedite resolution. Contractor will contact the facility to arrange for the on-site service at the convenience of the facility.

County facilities can also open and track trouble tickets through our convenient facility portal.

Facility Portal

At any time, day or night, 24x7x365, Maricopa County can securely access details about your facility's operations. Approved users can access all calling activity, including all call detail reports.

The Facility Portal can serve as the user interface to Contractor's electronic trouble ticket system and allows authorized users to perform functions such as creating and managing service tickets and generating reports. With Facility Portal, users can initiate trouble tickets for repairs, track the real-time status, and generate current and historical reports of these tickets. After a ticket is generated, a tracking number is automatically and immediately created. All updates are sent in real-time electronically to the originator of the ticket, as well as to the County designee.

Facility Portal Service Center

The Service Center will allow the user to create and manage their facility's technical support tickets. As needed, users can search for service tickets by entering the ticket number in the search field or by selecting date search

The Contractor Field Services Team

Each FST will be capable of completing a security screening prior to admittance to your facility. All field services support is provided to the counties in Wisconsin and throughout the United States by the Contractor team at no charge.

Field Service Technician Standards

Contractor's Field Services organization requires that all Field Services Technician (FST) personnel meet the following standards:

- **Are strategically located throughout the U.S.**— Our FSTs are located throughout the United States in strategic geographic locations that enable them to meet our clients' response time needs.
- **Meet educational and certification standards** — All FSTs are thoroughly screened before employment, and are required to have an extensive telecommunications background. Additionally, FSTs receive extensive Contractor's training and certifications to support our product offerings.
- **Receive product and engineering support** — Our in-house integrated support model keeps our technical support team engaged throughout problem resolution. FSTs and the technical support team have direct access to product and development engineers, enabling them to expedite repairs and minimize customer downtime.
- **Carry standard tools and parts** — All FSTs carry a complete set of tools and standard truck stock of parts to handle the majority of repair requests; these include telephone sets, handsets, dials, and replacement circuit boards, which they keep in their truck or on-site. If a technician does not have the spare part in his or her truck or at the site, Contractor will drop-ship the item to the site; or if the situation is critical, Contractor will ship counter-to-counter parts orders from our central warehouse on the same day.

The technician is required to follow a structured technical and management escalation process if they are unable to isolate the problem within four hours.

Field Service Manager

- Conduct remote visits via phone bimonthly. Based on information obtained from call, a trouble ticket may be opened
- Work with the account team to evaluate contract progress with the County quarterly
- Provide the facility with applicable site information that assists them based on the account profile.
- Monitor ticket traffic
- Resolve escalation issues, as needed

Each field service manager possesses the skills required to perform the duties of the field technician and can provide additional or backup support as needed.

- 4.5.2 The Contractor must provide all post installation system programming and maintenance services at no cost to MCSO
- 4.5.3 The Contractor must warrant that the Web-based Video Visitation/Communication Kiosk System installed for the MCSO facilities shall be free of defects, irregularities, unprofessional installation, code violations and shall operate as designed and proposed. Should the system not operate as designed and proposed or violate any local, state or federal code, the Contractor shall immediately correct the defect or irregularity or bring the system within code and performance specifications at no cost to MCSO.
- 4.5.4 Should any critical component of the Web-based Video Visitation/Communication Kiosk System provided by the Contractor fail, the Contractor must respond to Web-based Video Visitation/Communication Kiosk System maintenance/repair calls from MCSO in the manner outlined in this section.
- 4.5.5 Reporting Repair Problems – Describe the method of reporting repair problems. State whether or not MCSO will have access to the reports.

Maricopa County will use the Facility Portal to open and track trouble tickets, and to order marketing materials related to VVS. The Contractor-provided on site technicians will also support the facility by opening and tracking any service tickets through the Facility Portal. Although authorized personnel can generate reports themselves, the site administrators also will assist with any reports if needed by Maricopa County personnel.

Facility Portal

Contractor provides partnering facilities with one of the only anywhere, anytime single-point access customer portals in the industry. At any time, day or night, 24x7x365, Maricopa County can use our SCP user interface to securely access the facility's operations. Approved users can access all calling activity, including all call detail reports.

The Facility Portal can serve as the user interface to Contractor's electronic trouble ticket system and allows authorized users to perform functions such as creating and managing service tickets and generating reports. With Facility Portal, users can initiate trouble tickets for repairs, track the real-time status, and generate current and historical reports of these tickets. After a ticket is generated, a tracking number is automatically and immediately created. All updates are sent in real-time electronically to the originator of the ticket, as well as to the County designee.

- 4.5.6 Escalation List – Within 10 days of award of contract, provide a list of contact names, telephone numbers, and e-mail addresses for escalation of unresolved service requests and issues that are not resolved.

4.5.7 Service Availability - The contractor shall be available to service equipment and the Web-based Video Visitation/Communication Kiosk System when a priority level one or two service issue occurs 365 days per year without additional cost to MCSO. Priority level three services will be completed during regularly scheduled work hours, Monday through Friday.

4.5.8 System Checks – The contractor will perform system checks and preventative maintenance on a monthly basis to ensure the system is operating at optimum efficiency and performance. A system check and preventative maintenance logbook, that includes the findings and specified action, will be maintained by the Contractor and remain at a MCSO specified location.

Contractor proactively identifies potential system and network abnormalities through a centralized diagnostic application, Orion by Solar Winds. This network management software allows Contractor personnel to continuously monitor all hardware, software, and system metrics.

Through our network monitoring practices, we are able to complete the following functions:

- **Enable proactive repairs to a system to prevent it from going down.** Many times corrections are made before a system shows signs of an issue and before the facility is aware of a problem. This means less down time and increased system reliability for the facility.
- **Alert remote or on-site engineers of any system threshold inconsistencies or alarms.** If detected:
 - Alerts are sent to the NOC to track the event.
 - The NOC communicates with engineers through email, short message service (SMS), or directly through a wireless phone to address the issue.
- **Receive real time alerts when the system detects an error.**
 - Identifies if the network elements health threshold has been exceeded or if any other potential system issue has been discovered.
 - Establishes volume thresholds for each transport carrier on core node equipment at each data center, alerting Contractor personnel of possible carrier network issues.
- **Monitor call traffic patterns, bandwidth detail, and network life cycle management to ensure sufficient resources are in place.** A separate capacity engineering team reviews call traffic volume reports and storage requirements throughout all systems.
- **Centrally monitor all calling traffic and reporting to determine if increase or decreases in the number of telephones are needed.** Upon agreement by the County, the service and operations team will install any additional telephones required.

Remote Programming, Diagnostics, and Troubleshooting

The Contractor NOC uses the Orion network monitoring application to constantly check the system to ensure optimum performance and to anticipate the need for additional network or capacity.

Visual monitoring in our NOC is achieved through the use of several key screens that are constantly updated and monitored by our personnel in our NOC.

4.5.9 Kiosk Service Standards – Each instrument and phone enclosure shall be cleaned and wiped each time it is serviced, if needed.

- 4.5.10 Vandalism – Any act of vandalism or machine break-ins discovered by the Contractor shall be reported immediately to the Inmate Kiosk System Administrator, or his designee. The Contractor will be totally responsible for any loss due to acts of vandalism or other loss.

- 4.5.11 The Contractor must propose a Web-based Video Visitation/Communication Kiosk System that provides for remote diagnostics and maintenance.

The VVS solution is a Web-based, centralized system that allows for remote diagnostics and maintenance as well as automatic technology and feature upgrades. After the video visitation system has been implemented, it is easy for Contractor to enable new features and modules by activating the feature in the centralized system.

Designed to meet the needs of the facility *as defined by the facility*, Contractor Video Visitation offers both at-home and on-site solutions.

Contractor proactively identifies potential system and network abnormalities through a centralized diagnostic application, Orion by Solar Winds. This network management software allows Contractor personnel to continuously monitor all hardware, software, and system metrics.

- 4.5.12 System Failure –

Contractor' system failure backup plan is derived from our recovery plan for our phone systems, which are installed in about 2,200 locations across the nation.

Contractor will develop and maintain toll-free, 24-hour-a-day, 7-day-a-week emergency access phone number lists that will be readily available for use in any emergency situation. Contact information will be updated at regular intervals to ensure accuracy. Contractor' National Service Center will also maintain these emergency contact phone number lists and coordinate on a regular basis with field staff to ensure that all lists are accurate. In addition, Contractor will develop relationships with local vendors who can support emergency recovery operations with the required services, supplies, and equipment.

Technical Support

Contractor understands that throughout the duration of a critical event, our customers rely on our support to guide them with minimal loss of data and equipment. Qualified resources will be available to assist Maricopa County. These resources include the approximately 150 full-time field technicians who can deploy nationwide, and a full list of contacts—up to and including Contractor executives.

Contractor also realizes that during a disaster, it may be even more important that offenders and detainees can stay in contact with their friends and family. To support these end users, Contractor maintains two call centers in Dallas, TX, and Atlanta, GA, that can continue session processing, even if there is a failure at one location.

Coordination

Coordination of all declared emergencies will depend on the emergency level. Field staff will coordinate the emergency response to all level 3 conditions. Headquarters will provide assistance at the request of field management for Level 2 emergency conditions and will coordinate all Level 1 emergency efforts.

The field management team will develop mutual agreements with other Contractor regions in the country or with vendors to supply resources, equipment, or manpower. Additional equipment and personnel may not arrive for several days, depending on available transportation, condition of the roadways and airports, and other factors,

therefore field management will not delay the decision to ask for assistance from other sources.

Mobilization

Mobilization of a Headquarters Response Team, if necessary, will depend on need, as determined by the headquarters and field management.

The Headquarters Response Team will be dispatched from Dallas as soon as possible to assist field recovery efforts. However, field staff will begin recovery operations without delay.

Emergency Response Teams

Contractor will form the following teams to respond to declared emergency conditions. These teams will include subject matter experts and necessary support staff.

Table: Emergency Response Teams	
Team	Manning and Responsibility
Field Local Recovery Team	Plans and directs local recovery operations Staffed by field staff personnel only
Headquarters Support Team	Provides technical support and assistance to local recovery teams Staffed cross-functionally, as required
Headquarters Response Team	Deployed to Contractor local markets to assist local recovery operations The Headquarters Response Team is staffed by subject-matter experts and led by headquarters operations management

Recovery

Recovery operations may last several hours, several days, several weeks, or longer. Field staff will continue recovery operations until critical offender calling functions have been recovered and Contractor can restore phone service operations to normal call and data transmission capability. Senior Contractor management will, at that time, recall the Headquarters Response Team and field staff will return to normal operation. Recovery operations may still continue but emergency operations are no longer necessary and are not cost effective to maintain.

Throughout emergency recovery operations, the headquarters and field staff record all recovery actions. Following the resolution of emergency response operations, all recovery teams and appropriate management submit pertinent information and comments to be included in the Post Mortem report.

4.6 WARRANTY:

The contractor shall provide 100% warranty for the software and hardware of the Web-based Video Visitation/Communication Kiosk System for the duration of the contract at no cost to MCSO.

4.6.1 The Contractor is responsible for replacement of the Web-based Video Visitation/Communication Kiosk System in its entirety or its individual components

regardless of cause including, but not limited to, normal wear and tear due to regular use, inmate abuse and inmate unrest, and natural or man-made disasters including cyber-attacks and/or cyber-terrorism. This system or component replacement will be performed at no cost to MCSO and will occur immediately upon notification to the Contractor of the system problem by MCSO facility. The Contractor must replace visitation kiosks requiring repair and not repair components of the visitation kiosks on site at MCSO.

4.7 TRAINING:

4.7.1 Initial Training - The contractor shall provide training to familiarize all MCSO personnel with the Web-based Video Visitation/Communication Kiosk System.

VVS training covers all current system features and will provide additional training as more are added and the system enhanced. Contractor uses our own experienced employees to conduct all training through online instructor-led classes or on-site, one-on-one and classroom training sessions at no cost to you. Standard training includes using both hands-on experience with your data and using instructor demonstrations to ensure each trainee understands all VVS concepts.

Contractor training programs enable facility staff to use all features the first day of installation. Since products are Web-based, after a two- to three- hour training session most officers find it easy to maneuver through the features immediately.

In addition to standard training, Contractor will work with Maricopa County to customize your online training experience to meet the unique needs of your staff and facility. We offer separate classes focused on different agency functions such as, creative investigations, well-organized live call monitoring, and efficient system administration. Training for product upgrades, new facility staff, or a general refresher course is offered through online instructor-led courses available twice a month throughout the year—*Contractor ongoing training ensures your staff always "stays on top" current and newly released VVS features.*

VVS Training Course Modules

Contractor is committed to providing your staff with training that will maximize the potential of the features implemented at your facility. Training courses are in a user-friendly, task-oriented format to teach your officers what they need to know to do their job. We present courses in separate modules based on the types of duties officers tend to perform using the SCP inmate telephone system while expressing the unique features of applications.

The following table presents the standard SCP training course modules and associated learning objectives.

VVS Course Modules

Course Module	Objective
Overview and Navigation	<ul style="list-style-type: none"> • User types • Appointment types • Process flow • URL - status bar - webcam • Internet speed - storage term • Three main modules

Course Module	Objective
Appointments	<ul style="list-style-type: none"> • Stop or cancel a session • Change date/time • Change terminal • Live monitor sessions
Administration	<ul style="list-style-type: none"> • Users and user groups • Terminals and locations • Logs
Session Viewer	<ul style="list-style-type: none"> • View a recorded session • Actions and icons - search, play, lock, delete
Visitation Schedule	<ul style="list-style-type: none"> • Customized by user type
Optional Applications	<ul style="list-style-type: none"> • Sick Call - symptoms • Commissary Ordering • Automated inmate information

- 4.7.2 The Contractor must provide all end-user training to the MCSO at no cost.
- 4.7.3 The Contractor must provide all end-user training on site at the various MCSO facilities.
- 4.7.4 The Contractor must provide training for various levels of MCSO personnel including full-time system administrators, part-time system administrators, special investigators, and data entry specialists, etc.
- 4.7.5 The Contractor must provide full training for all assigned system users on how to create, delete and modify inmate programming and profiles.
- 4.7.6 The Contractor must provide full training for all assigned system users on how to generate appropriate system reports.
- 4.7.7 The Contractor must provide full training for all assigned system users on how to maintain inmate alert levels and respond accordingly when these levels are exceeded.
- 4.7.8 The Contractor must provide full training on the provided video visitation recording function including the live monitoring of visitation sessions, playback of visitation sessions and the transfer of visitation sessions to other media for playback at off-site locations.
- 4.7.9 The Contractor shall provide full training for all assigned MCSO system users on how to change inmate restriction levels (by kiosk, suspend PIN, etc.).
- 4.7.10 The Contractor must provide full training for all assigned system users on how to initiate system restrictions.
- 4.7.11 The Contractor must provide ongoing system training for existing MCSO personnel when required by the MCSO at no cost.
- 4.7.12 The Contractor must provide additional training for new MCSO personnel when required by the MCSO at no cost.
- 4.7.13 The Contractor must describe, in its response, any advanced system training that may be available to MCSO personnel whether provided on-site at the MCSO facility.
- 4.7.14 The Contractor must provide a "live" Help Desk support function to MCSO at no cost to the MCSO during the term of this contract. This Help Desk function must be capable of

providing support via telephone to the MCSO Web-based Video Visitation/Communication Kiosk System personnel for the functions of the Web-based Video Visitation/Communication Kiosk System. This "live" Help Desk must be available 24 hours a day, 7 days a week, 365 days per year.

- 4.7.15 User Manuals – The contractor shall provide user manuals, both printed and electronic versions, for their platform to MCSO in sufficient number as deemed necessary by the Sheriff's Training Center.

4.8 REPORTS:

- 4.8.1 Ability to Customize Special Reports – The system may provide the capability to customize reports in a form mutually agreed upon by MCSO.
- 4.8.2 Finance Reports – The contractor shall list any and all reports available. Include an example of the reports. These should include revenue and commission by jail facility and category.
- 4.8.3 Maintenance Reports – Contractor shall grant County access to an online reporting portal that shall include the following report types:
 - 4.8.3.1 Kiosk Repairs
 - 4.8.3.2 Web-based Video Visitation/Communication Kiosk System Trouble Tickets
 - 4.8.3.3 System Upgrades
- 4.8.4 Inmate Reports – The contractor shall list any and all reports available and include an example of each report. (An example would include video specific to one inmate by time and date.)
- 4.8.5 IP Number Reports – The contractor shall list any and all reports available and include an example of each report. (Examples may include blocked IP numbers, IP numbers visiting more than one inmate, and frequently used IP numbers.)
- 4.8.6 Web Video Access Reports – The contractor shall list any and all reports available and include an example of the reports.
- 4.8.7 Investigative Reports – The contractor shall list any and all reports available and include an example of each report.
- 4.8.8 Inmate Email Reports- The contractor shall list any and all reports available and include an example of each report.
- 4.8.9 Inmate Tank Order Reports- The contractor shall list any and all reports available and be able to differentiate between requests (i.e. programs, religion, library, ILS). Include an example of each report.
- 4.8.10 Disciplinary Action Reports- The contractor shall list any and all reports available and include an example of each report.

4.9 PERFORMANCE SPECIFICATIONS:

Disputes/Fines/Assessments – MCSO expects the contractor to fully comply with the time frames in this contract. However, should a dispute arise as to whether there should be a fine for non-compliance and if so, how much, the dispute will be resolved by a team consisting of two (2) members from MCSO, one (1) member from Maricopa County Office of Procurement Services Department and one (1) member from each of the contractors service team. Each dispute resolution team member will have one vote with the exception of the service provider team

member whose company is being considered for assessment of the fine. This exception team member may represent his company's position during the discussions. A simple majority shall be required of the eligible voting dispute resolution team members to determine the resolution. The decision will be based on the logbooks, work orders, e-mails, and written explanations from all parties involved in the dispute. The final decision of the dispute resolution team will be final and binding upon all parties.

- 4.9.1 Jail Facility Access Security Clearance - MCSO does not allow a service contractor access into a jail facility to perform any type of service unless a background check has been completed, per Exhibit 7 Jail Access Policy. The MCSO Facilities Security Guidelines (Exhibit 7) explain all the necessary requirements of contractors performing work at such facilities. If it is anticipated that the contractor has staff visiting the site on a consistent basis, these forms will be completed by the person requesting facility access and the background check will be completed prior to approving access. Once the form is filled out and submitted to MCSO, the contractor shall be notified if approved and a jail access identification card will be issued.
- 4.9.2 Security of Records/Recordings – The contractor shall provide adequate security of the inmate Web-based Video Visitation/Communication Kiosk System records and recordings. Access to the Web-based Video Visitation/Communication Kiosk System records and recordings will be limited to those employees of the contractor who requires the information to properly perform services for MCSO.

Contractor provides multiple safeguards, both at a user and facility level, to ensure the highest amount of security for at home visitation. In addition to a registration process which requires end users to enroll and take verification photographs of their identification and profile, which must be approved prior to a visit being scheduled, Contractor takes the following steps to ensure security:

- Video security screens which do not permit viewing at an angle
- Hardened glass on terminal screens to minimize breakage and downtime
- Ventilated and cooled video monitor hardware without providing inmates areas to "stuff" items
- Magnetic on and off switch to prevent inmate tampering
- Vandal proof handset with armored cable
- Assembly elements are hidden: No screws or hinges can be removed and used to manufacture weapons. No doors/compartments that can be opened in the front or on the sides of the unit
- Rounded edges that reduce the risks of accidental or intentional injuries
- Abrasion and chemical resistant; can be cleaned with commercial cleaners without damage
- Live monitoring capabilities of real-time visits
- Recording of visits for security purposes
- Impact Resistance - Meets UL-60950 and CSA 22.2 No. 60950 ball drop test (0.5kg, 50mm diameter ball dropped from height of 1.3m)
- Screen size is 15"
- Terminal has steel, mounting bracket which is bolted to the wall. Afterwards, the terminal is secured to the bracket.
- Light and ruggedized vandal-proof terminals (constructed with hardened, cold rolled steel .075/14 gauge): Best balance between weight and resistance
- Terminal is sealed: Minimize dust and liquid entry, spill proof, completely sealed front, spill-resistant back with openings to allow heat to escape.
- Hidden magnetic activated pushbutton for on/off power
- Built-in heat sink at the back for heat dissipation

- Power: 110V; 2AMP
- All content is delivered via web browser through servers hosted in Contractor' data centers.

In addition, the Maricopa County's VVS network will operate on Contractor' secure, private network.

Contractor understands the importance of security, particularly in the corrections industry and takes security concerns seriously.

Contractor applies a high level of security to protect against cyber-pirates. Applications transmitting data across public networks are supporting SSL, Certs, and encryption. Cisco and Juniper firewalls, used throughout the network to protect SCP and our customers, create DMZ networks. In addition, all servers, laptops, and workstations require anti-virus and anti-spyware protection software, and the latest operating system patches. Contractor supports both AVG and Symantec anti-virus.

From a physical security standpoint, VVS is co-located in a carrier-class data center that has some of the most comprehensive security measures in the telecommunications industry. Access to network facilities is controlled through multiple levels of mandatory physical security.

Security personnel maintain the following procedures for allowing entry into the data centers:

- Security personnel are on premise 24x7x365.
- Cardkey reader (electronic badge).
- Identification badges are issued to all persons having a business need to access Company premises.
- Man traps are located at each entry/exit point in the data center. Man traps use two sets of doors that require electronic badge entry. The first set of doors must close before the second set will open.

All visitors, customers, contractors, and repair personnel must gain access from the security officer on duty.

Customers, contractors, repair personnel, maintenance personnel, and non-local employees may access buildings and critical areas at all times, if there is an escort. Vendors may access buildings and critical areas only during working hours, if there is an escort.

As Contractor has demonstrated with over 25 years of call platform enhancements, we will continue to reinvest in our video platform over the term of our relationship to implement features driven by our customers. As new advances in security are made available, we will provide them to Maricopa County.

- 4.9.2.1 Procedures and Controls - The contractor shall establish and maintain procedures and controls that are adequate to assure that no information contained in its records and/or obtained from the Sheriff's Office or from others in carrying out the functions/service under this Agreement shall be used by or disclosed by it or its employees, except as required to efficiently perform duties under the Agreement.
- 4.9.2.2 Records/Recordings Confidentiality – Contract employees that have access to the inmate telephone records and recordings shall be required, at a minimum, to sign a Non-Disclosure/Confidentiality Agreement and potentially the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum Certification.
- 4.9.2.3 Records/Recordings Security Clearance – Contract employees that have access to the inmate video records and recordings shall be required to

complete, at a minimum, a background check and potentially a fingerprint check.

4.9.2.4 Legal Video/Web-based Visitation shall not be recorded without a court order.

4.9.3 Trouble Ticket Fines

4.9.3.1 Priority Level One (1) Fine: A fine of \$500.00 shall be assessed to the contractor for every day in which a Priority Level One (1) Trouble Ticket has not been resolved and the service is not fully restored to the affected areas.

4.9.3.2 Priority Level Two (2) Fine: A fine of \$250.00 shall be assessed to the contractor for every day in which a Priority Level Two (2) Trouble Ticket has not been resolved and the service is not fully restored to the affected area.

4.9.3.3 Priority Level Three (3) Fine: A fine of \$100.00 per day shall be assessed to the contractor for every day in which a Priority Level Three (3) Trouble Ticket has not been resolved and the service is not fully restored to the affected area. A 48-hour grace period will apply.

4.9.4 Compliance of Jail Access Rules and Regulations – The contractor shall comply with all provisions outlined in MCSO Policy DH-1, Jail Access (Exhibit 7).

4.9.5 Staffing

4.9.5.1 On Site Technicians - The contractor shall provide three (3) full-time “on-site” technicians at their expense to provide service. The technicians must have at least two (2) years of related experience, to include installing, maintaining, testing, and repairing voice and data communications systems and equipment. The duties include:

4.9.5.1.1 Repair and Maintenance – The contractor shall provide service for all Web-based Video Visitation/Communication Kiosk System repair and maintenance.

4.9.5.1.2 Video Party Billing Issues – The contractor shall handle all billing issues from the parties called by the inmates.

4.9.5.1.3 Complaints – The contractor shall handle all complaints from the parties for web-based issues.

4.9.5.2 Trained Support Staff - The contractor shall maintain properly trained support staff on the Web-based Video Visitation/Communication Kiosk System.

4.9.5.3 Compliance of Code of Conduct for On Site Technicians - The On-Site Technicians shall comply with all provisions outlined in MCSO Policy CP-2 Code of Conduct (Exhibit 6).

4.9.5.4 Replacement of On-Site Technicians – The contractor shall replace any on-site administrator who leaves employment with the contractor, within twenty-one (21) days. This replacement may be a temporary or permanent employee. If the replacement is a temporary employee, a permanent employee (full or part-time) will be hired by the contractor and on site within sixty (60) business days of the date the previous employee left employment of the contractor.

4.9.5.4.1 Fine – Failure to comply shall result in a \$250.00 fine per day until the contractor is in compliance.

- 4.9.6 Service Point of Contact – The contractor shall provide a complete list of business telephone numbers, emergency telephone numbers, addresses, and e-mail addresses of the contractor's managers, administrators, and technicians within ten (10) days of the award of the contract.
- 4.9.7 Public Complaints Point of Contract – The contractor shall provide a single point of contact for any and all public complaints regarding telephone service. This service must be provided for both English and Spanish speaking individuals.
- 4.9.8 Complaints of or by Contracted Employees – The contractor shall investigate any complaints of or by contracted employees and have resolution within thirty (30) days with notification of such to MCSO.
- 4.9.9 Office Equipment – Any office equipment, desks, cell phones, pagers, etc., required by the contractor's personnel shall be the responsibility of the contractor.
- 4.9.10 Remote and On-Site Monitoring – The contractor shall provide to MCSO on-site monitoring during normal business hours and remote monitoring and diagnostic service, twenty-four (24) hours a day, seven (7) days a week.
- 4.9.11 System Checks and Preventative Maintenance – The contractor shall perform system checks and preventative maintenance on a monthly basis to ensure the system is operating at optimum efficiency and performance.
- 4.9.12 Coordination of Services – All changes in present and future services shall be coordinated with the Web-based Video Visitation/Communication Kiosk System Manager, or designee.
- 4.9.13 Coordination of Maintenance – All operational maintenance shall be coordinated with the Web-based Video Visitation/Communication Kiosk System Manager, or designee.
- 4.9.14 Kiosk Cleaning at Time of Service – All exterior of equipment as well as interior and exterior enclosures shall be cleaned at the time of each service. Labels or information cards will be replaced when missing or damaged.
- 4.9.15 Clean Up and Debris – The contractor shall clean up and remove all debris and packaging material resulting from work performed.
- 4.9.16 Project Plan – The contractor shall provide a detailed project plan, including a Gantt Chart, stating all tasks, milestones, and target dates for the initial project.
- 4.9.17 Statement of Work – The contractor shall provide a statement of work and obtain MCSO approval for any and all software changes prior to the installation of the software change.
- 4.9.18 Installation, Replacement, and Repair Cost – The contractor shall be responsible for installation, replacement, and repair cost of all equipment due to any reason including, but not limited to, vandalism, normal wear and tear, and new installation requirements.
- 4.9.19 Cost of Installation, Monthly Usage and Maintenance of Kiosks – All expenses involved with the installation, monthly usage, and maintenance of the contractor-installed telephone lines shall be borne solely by the contractor.
- 4.9.20 Credit and Collection Practices – The contractor shall adhere to reasonable credit and collection practices.
- 4.10 SYSTEM UPGRADES
 - 4.10.1 In the event that a system upgrade needs to take place that will impact the operation of the system, the Contractor shall:

4.10.1.1 Notify County at least one week prior to the event

4.10.1.2 Not allow system disruption outside of the hours of 2200 and 0600 Arizona time in order to avoid the cancellation and or delay of scheduled activities

4.10.1.2.1 If this cannot be accomplished, Contractor representative shall:

4.10.1.2.1.1 Be in immediate communication with County and provide County with a detailed explanation of the failure.

4.10.1.2.1.2 Provide County a corrective action plan detailing specifically what actions or processes the Contractor has implemented in order to avoid a recurrence of the failure. Said report shall be delivered no later than one week post the failure date.

4.10.1.2.1.3 Contractor shall have the responsibility for contacting all impacted external customers and arranging for alternate visitation.

EXHIBIT C

CODE OF CONDUCT POLICY

	MARICOPA COUNTY SHERIFF'S OFFICE	
	Policy & Procedure	Joseph M. Arpaio – Sheriff
	Subject	Policy Number
	CODE OF CONDUCT	CP-2
		• Effective Date 03-28-12
Related Information	Supersedes	
CRITICAL POLICY	CP-2 (02-06-04)	

PURPOSE

The purpose of this Policy is to establish guidelines by which all employees of the Office shall conduct themselves, both on and off duty.

Although this Policy refers to “employees” throughout, this Policy also applies with equal force to all volunteers. Volunteers include, but are not limited to, reserve deputies and posse members.

Note: The number of topics covered on the following pages justifies the use of an alphabetical index that can be found at the end of this Policy.

POLICY

It is the policy of the Office to ensure efficiency, instill discipline, and foster positive public trust by setting forth guidelines governing the conduct and demeanor of every member of the Office. This Policy is also intended to hold employees accountable for federal, state, and local laws by ensuring that any criminal misconduct is investigated.

DEFINITIONS

Employee: A person currently employed by the Office in a classified, unclassified, full-time, part-time, contract, or probationary status.

Negligence: Failure to use ordinary care.

Relative: An employee’s spouse, domestic partner, mother, father, sister, brother, son, daughter, in-laws, aunts, uncles, grandparents, grandchildren and custodial person.

Volunteer: A person who performs hours of service for civic, charitable, or humanitarian reasons, without promise, expectation, or receipt of compensation for services rendered. An employee may not volunteer to perform the same, similar, or related duties for the Office that the employee is normally paid to perform.

Willful: An action taken deliberately or intentionally.

PROCEDURES

1. **Unethical Conduct:**

- A. Employees shall maintain a high level of ethical conduct at all times and shall be honest, fair, impartial, and polite when working or identified as employees of the Office.
- B. Employees shall not participate in any activity which would compromise their ability to perform their Office duties objectively and impartially.
- C. Personnel shall not withhold relevant information or mislead investigators during a criminal or administrative investigation.
- D. All employees shall abide by the *Sheriff's Office Code of Ethics*, as specified in this Policy. Classified Employees shall also abide by the Maricopa County Merit System Rules Code of Ethics.

2. **Conformance to Office Directives and Established Laws:**

- A. Employees shall conform to the provisions of all written Policy, except those found to be unlawful, incorrect, or inapplicable. Violation of written Policy, with or without articulable justification, may result in disciplinary action.
- B. Employees shall obey all local ordinances as well as all federal and state laws. Violation of any established ordinance or law may result in disciplinary action being imposed, in addition to the possibility of criminal prosecution. Disciplinary action may be imposed regardless of the outcome of the court case.
- C. Employees shall be held fully accountable for their own acts. They shall not shift the burden or responsibility to another for their failure to execute an order or duty, for inappropriate behavior, or for any other dereliction of duty.

3. **Individual Responsibility:** To ensure the credibility and integrity of the Office, it is the duty of all personnel associated with the Office to take appropriate action whenever they learn of a violation being committed, or having been committed, by any other person associated with the Office in any capacity, which by its very nature would tend to discredit an employee or the Office.

- A. Personnel shall bring any and all facts concerning an actual or alleged violation to the immediate attention of an on-duty supervisor or an appropriate commander.
- B. The on-duty supervisor or commander shall then initiate the appropriate action after considering all of the facts presented and the seriousness of the allegation.
- C. Personnel shall not retaliate against an employee who reports misconduct or a violation in fulfillment of this individual responsibility or duty.

4. **Unbecoming Conduct and Public Demeanor:**

- A. Employees shall conduct themselves at all times, both on and off duty, in such a manner as to reflect favorably on the Office. Unbecoming conduct shall include disorderly conduct and activities that conflict with, or have the potential to conflict with, Office duties; tend to bring the Office into disrepute; reflect discredit upon employees as

members of the Office; or tend to impair the operation and efficiency of the Office or any of its employees.

- B. Employees shall show respect for the uniforms of the Office at all times. When worn, all uniforms shall be neat, clean, and worn in compliance with Policy GC-19, *Dress and Appearance*. No distinguishable portion of the uniform shall be worn with civilian attire or any other uniform, on or off duty, as specified in Policy GC-20, *Uniform Specifications*. At no time shall any Office uniform be worn to represent the wearer as having the authority of any other class of employee.
- C. Employees who are on duty or identified by dress, location, or association as employees, shall maintain a professional demeanor and perform their duties in a calm and firm manner, acting together to assist and protect each other.
- D. Employees shall not demean persons or act disparagingly against any individual regardless of age, nationality, religious beliefs, race, gender, culture, sexual orientation, veteran status, ancestry, or disability.
- E. Employees shall conduct themselves in a manner that will foster respect and cooperation among themselves and other members of the Office.
- F. Employees shall not, at any time or for any reason, subject any person to cruel treatment or neglect humane action.
- G. Employees shall not, at any time or for any reason, subject any animal to cruel treatment or neglect humane action. Hunting, when it is conducted according to law, shall not be considered a violation of this section.
- H. Employees who have contact with the public should strive to gain public support and citizen cooperation by dealing with people fairly, honestly, and courteously.

5. **Alcohol:**

- A. Except in the performance of official duties or authorized training and with prior supervisory consent, employees shall not purchase or consume any kind of alcoholic beverage while on duty. Additionally, employees shall not report for duty, or be on duty, with any odor of alcoholic beverage on their breath or while under the influence of any alcoholic beverage to any degree. Any employee observing another employee in violation of this section shall advise any on-duty supervisor as soon as possible. Impairment is not requisite for violations of this section.
- B. A supervisor who reasonably believes that an employee who is on duty or reporting for duty smells of, or is under the impairment of, alcohol to any degree, shall refer to the procedures specified in Policy GC-21, *Drug, Medication and Alcohol Testing*.
- C. Employees authorized to consume alcoholic beverages in the performance of their duty, such as undercover detectives, shall comply with the provisions of Policy ED-2, *Covert Operations*. In all cases, personnel who consume alcoholic beverages on duty shall avoid any physical condition or impairment which could adversely affect their performance of duty or bring discredit upon the Office. Supervisors of such employees are cautioned that they are responsible for monitoring the conduct and demeanor of personnel engaged in the consumption of alcoholic beverages and taking appropriate action.
- D. Office personnel in specialized assignments who are subject to call out are requested to refrain from alcoholic beverage consumption.

1. If called out, an employee who has been drinking within the last eight hours shall advise his immediate supervisor, if available, or the on-duty supervisor that he has been drinking, the type and amount of alcohol consumed, and how long it has been since his last drink.
 2. Based on the information provided by the employee, the supervisor shall consider all factors, including the time elapsed, when making a decision to activate an employee who has been drinking. Based on the totality of the information, the supervisor's decision must be made to ensure that the employee has not consumed any alcohol within the last eight hours.
- E. Employees shall not operate any County vehicle within eight hours after consuming any alcoholic beverage. Employees working covert operations shall adhere to the procedures specified in Policy ED-2, *Covert Operations* regarding the consumption of alcoholic beverages and operating a County vehicle.
- F. On and off-duty employees shall not display or wear any recognizable item of Office apparel in a public place or an establishment where the primary purpose is to sell or serve alcoholic beverages, unless in the performance of official duties.
- G. Employees shall not consume alcoholic beverages in any County facility or County vehicle except in the performance of official duties or authorized training and with prior supervisor consent. Employees, their guests, volunteers, citizen observers, or other citizens are prohibited from consuming alcoholic beverages at any time, or for any reason, while in County facilities or County vehicles. Employees observing violations shall promptly report the violation to a supervisor who will take action to stop the violation.
6. **Use of Medication or Drugs:**
- A. Employees are prohibited from using any drug which has not been legally prescribed for their use, or abusing prescription or over-the-counter medications. Any use of drugs not legally prescribed for the employee's use, or any abuse of prescriptions or over-the-counter medication, shall be grounds for discipline, up to and including dismissal from employment.
- B. Employees who take prescribed or over-the-counter medications are responsible for being aware of any effects the medications may have on the performance of their duties. Employees shall advise their supervisor, prior to reporting for duty, when taking medication that might impair their ability to perform the essential job functions of their position. The employee shall provide his supervisor with a written memorandum identifying the essential job functions that may be affected as a result of any side effects from the medication. The employee shall also include the anticipated amount of time the medication is to be taken or the date it is believed that it will no longer be needed.
- C. A supervisor who reasonably believes that an employee who is on duty, or reporting for duty smells of, or is under the impairment of, drugs or medication to any degree, shall follow the procedures specified in Policy GC-21, *Drug and Alcohol Testing*.

7. **Gratuities, Rewards, or Loans:**

- A. Employees will not use their position for personal gain, on or off duty, nor solicit, seek, or accept on their own behalf any personal loan, gift, gratuity, or other favor, from the general public, any private business firms which deal with the Office, or any other agency or department of the County which is, or may appear to be, intended to influence official conduct. Discounts and offers which comply with and are authorized under a County or Office solicitation policy are exempted from this provision.
 - 1. This section does not prohibit the acceptance of food or refreshments of insignificant value in the ordinary course of a meeting, conference, or other occasion where the employee is properly in attendance.
 - 2. This section does not prohibit the acceptance of unsolicited advertising or promotional material such as pens, pencils, calendars, and other items of nominal value.
 - 3. This section does not preclude an employee from accepting off-duty work.
 - a. All off-duty work obtained must meet the requirements of Policy GC-18, *Off-Duty Employment*.
 - b. The off-duty employment must not place the employee as an expert witness against the Office or opposing any other criminal justice agency, including occupations such as a traffic reconstruction consultant.
- B. Employees shall not accept, directly or indirectly, a gratuity, fee, loan, reward, or gift of any kind for services rendered in the course of official duties or for services rendered in the course of an Office-approved off-duty assignment. This includes directly or indirectly accepting or obtaining a gratuity, fee, loan, reward, or gift of any kind and passing it on to relatives, friends, other Office employees, or acquaintances.
- C. Employees shall not use their position to solicit free admission to places of amusement, entertainment, or sporting events, or to solicit free meals or any favors or gratuities not ordinarily afforded to a private citizen.

8. **Compensation:** Pursuant to ARS §38-505, no public officer or employee may receive or agree to receive, directly or indirectly, compensation other than as provided by law for any service rendered or to be rendered by the employee personally in any case, proceeding, application or other matter pending before the Office of which he is a public officer or employee. Compensation is statutorily defined as money, a tangible thing of value, or a financial benefit.

9. **Abuse of Position or Authority:**

- A. Employees are prohibited from using their official position, identification cards, or badges for any of the following:
 - 1. Personal or financial gain.
 - 2. Obtaining privileges not otherwise available to them or to others, except in the performance of duty.

3. Avoiding the consequences of illegal acts such as traffic violations or driving under the influence, or helping relatives or friends avoid the consequences of illegal acts.
 4. Misrepresenting their position or authority in the Office.
- B. Employees shall not lend their identification cards, badges, or uniforms to another person. Employees shall not permit their identification cards or badges to be photographed or reproduced unless necessary for official business such as extradition trips, obtaining records from other government agencies, or otherwise authorized by the Chief Deputy.
- C. Employees shall not identify themselves as members of the Office, visually or verbally, in connection with testimonials or advertisements, unless specifically authorized by the Chief Deputy.
10. **Care and Use of Office or County Equipment:**
- A. Employees shall use Office and County equipment for its intended purpose. Limited incidental personal use of Office and County cell phones, fax machines, printers, and copiers are permitted. Such use shall not inhibit either governmental or administrative use or impact employee's ability to perform their assigned duties. Email and voicemail are authorized for limited incidental personal use as specified in Policy GM-01, *Electronic Communications and Voice Mail*.
- B. Office and County equipment shall not be willfully or negligently damaged, lost, misplaced, or abused. All equipment issued to employees shall be maintained in proper order.
11. **Confidential Information, Protected Health Information, and Divulging Criminal Records:**
- A. Employees shall only discuss or disclose sensitive law enforcement or confidential information as follows:
1. As permitted or required by law.
 2. With persons authorized to receive the information.
 3. As directed by a supervisor.
- B. In the course of official business, employees may learn certain facts that are of a personal or confidential nature regarding an employee, inmate, or other person's health or medical information.
1. Employees shall not use, copy, make notes regarding, remove, release, or disclose this information unless doing so legally in the course and within the scope of their official duties.
 2. Employees who become aware of anyone improperly accessing or releasing this information shall immediately notify a supervisor.
- C. Employees shall not release Criminal History Record Information (CHRI) on any individual, except as provided in Policy GF-3, *Criminal History Record Information and Public Records*.

12. **Performance or Dereliction of Duty:** Employees are derelict in the performance of their duties when they willfully or negligently fail to perform them or when they perform them in a grossly inefficient manner.
 - A. Employees shall devote their working time and attention to the service of the Office and shall complete all assignments in a timely manner, as set forth by their supervisor or chain of command.
 - B. While on duty, employees shall not engage in any activities or personal business, such as personal phone calls, which would cause them to neglect or be inattentive to duty.
 - C. Employees shall serve the Office with loyalty and discretion and shall not display cowardice or fail to support their fellow employees in the lawful performance of duty.
 - D. Judicial subpoenas shall constitute an order to appear and shall be honored, whether on behalf of the state or in actions against the employee, as governed by Policy GD-9, *Receipt of Civil or Criminal Process*.
 - E. Employees shall not engage in any strike. The term "strike" includes a concerted failure to report for duty, willful absence from one's position, or the stoppage of work. It also includes unauthorized holidays; sickness unsubstantiated by a licensed health care provider's statement during a strike situation; or withholding the full, faithful, and proper performance of the duties of employment for the purposes of inducing, influencing, or coercing a change in rights, conditions, compensation, privileges, or obligations of employment. Employees who engage in any strike shall be disciplined, up to and including dismissal from employment.
13. **Punctuality:**
 - A. All employees shall be punctual in reporting to their designated duty post and shall be physically ready to assume their duties at the time specified by their supervisor.
 - B. Foreseeable tardiness must be approved in advance to ensure proper staffing of the Office. Unless circumstances are of an emergency nature, any unforeseeable tardiness must be reported to the employee's supervisor no later than 15 minutes before the start of the shift. Unless the supervisor has issued a memo detailing another notification option for subordinates, an employee who is late for work must either call and speak to the supervisor, or leave a voicemail message for the supervisor with current contact information where the employee can be promptly reached.
 - C. Employees and supervisors should refer to Policy GC-1, *Compensation, Leaves, and Absences*, for information regarding foreseeable and unforeseeable absences.
14. **Political Activity:** It is the intent of the Office to conform to the public policy that government programs be administered in an unbiased manner and without favoritism for or against any political party or group or any member in order to promote public confidence in government, government integrity, and the efficient delivery of governmental services and to ensure that employees are free from any express or implied requirement or any political or other pressure of any kind to engage or not engage in political activity.
 - A. Employees shall not use the authority of their positions to influence the vote or political activities of any subordinate employee. Furthermore, under the guise of County business,

personnel, equipment, materials, buildings or other resources shall not be used for the purpose of influencing the outcomes of elections.

- B. Employees shall not use political endorsement in connection with any appointment to a position in the County classified service.
- C. Employees shall neither use, nor promise to use, any official authority or position for the purpose of influencing the vote or political action of any person or for any other considerations.
- D. No person may solicit any employee to engage in, or deny him the opportunity to engage in, activities permitted by this section. Any direct or indirect threat, such as intimidation, coercion, discrimination, reprisal, force, or any adverse consequence, such as the loss of any benefit, reward, promotion, assignment, or compensation, is prohibited.
- E. Except for voting, employees shall not engage in any activity permitted by this section while on duty, while in uniform, or at public expense. Nothing in this Policy shall be construed as denying any employee of any civil liberties as guaranteed by the United States or Arizona Constitutions.
- F. Employees shall not be members of any national, state, or local committee of a political party, nor an officer or chairperson of a committee of a partisan political club, nor a candidate for nomination or election to any public office, which is either paid or partisan. They shall not take part in the management of any political party, partisan or nonpartisan campaign, or recall effort.
- G. The provisions of this section shall not apply to school board or community college district governing board elections. An employee may serve as a member of the governing board of a common or high school district, or as a member of the community college governing board.
- H. While off duty, employees may:
 - 1. Express opinions, attend meetings for the purpose of becoming informed concerning the candidates for public office and the political issues, cast a vote, and sign nominating or recall petitions.
 - 2. Make contributions to candidates, political parties, or campaign committees contributing to candidates, or advocate the election or defeat of candidates.
 - 3. Circulate candidate nomination or recall petitions, or engage in activities to advocate the election or defeat of candidates.
 - 4. Solicit or encourage contributions to be made directly to candidates or campaign committees contributing to candidates, or advocate the election or defeat of candidates.
 - 5. Campaign for themselves and hold unpaid, nonpartisan public office, or campaign for or against ballot issues, referendum questions, constitutional amendments, or municipal ordinances, except where a conflict of interest is created.
- I. No employee shall be discriminated against for engaging in, or choosing not to engage in, any activity permitted in this section.

- J. Any person in the County service who violates any of the provisions of this section shall be subject to disciplinary action, up to and including dismissal from employment.
 - K. Employees who have relatives running for political office shall ensure that their conduct in support of their relatives is consistent with the provisions of this section.
15. **Public Appearances and Statements:** Any public expression, by which it could be reasonably assumed that the employee is acting as a spokesperson on behalf of the Office, will be governed by this Policy.
- A. Employees shall not publicly ridicule the Office, its Policies, or its employees, orally or in writing, where such expression is defamatory, obscene, unlawful, tends to undermine the effectiveness of the Office, interferes with the maintenance of discipline, or is made with reckless disregard for the truth.
 - B. Employees shall not address public gatherings, appear on radio or television, or release for publication an article, manuscript, or other material which pertains to the operations or activities of the Office without prior approval from their bureau commander. To be authorized, such articles, manuscripts, and interview materials must support the Mission Statement of the Sheriff's Office and reflect Office goals and objectives.
 - C. Employees shall not act in a private capacity or do any work in a private capacity, which may be construed by the public to be an official act of the Sheriff's Office, without prior written approval of the Chief Deputy.
16. **Endorsements, Referrals, and Vendors:**
- A. Employees acting in their official capacity must comply with County and Office procurement procedures. As a result, employees shall not recommend, suggest, or advocate for the employment or procurement of any particular product, professional, or commercial service outside the official procurement process. When any such service is necessary, employees shall proceed in accordance with GE-1, *Supply Requisition, Procurement, and Inventory*.
 - B. Employees must disclose their interest and shall not participate in or vote for any contract, sale, purchase, or service in which they have an interest. Conflict of interest laws must be observed.
17. **Labor and Fraternal Organizations and Associations:** Employees may join and hold office in any employee organization, labor union, or professional association in which they are eligible for membership, provided it is not organized for any illegal purpose or primarily engaged in activities contrary to law. No employee shall attempt to prohibit or intimidate any covered employee from belonging to or holding office in any lawful organization. Membership in such organizations shall not be considered in any personnel action, including promotion, demotion, suspension, or dismissal from employment.
18. **Associations and Fraternization with Inmates or Prisoners:**
- A. Employees shall not indulge in undue familiarity with inmates or prisoners. Employees shall not fraternize with, engage the services of, accept services from, or do favors for, any person known to them to have been in the custody of the Office or any other detention or correctional facility within the last two years, unless it is unavoidable due to relative relationships.

- B. Employees shall not convey written or oral messages between inmates, except those which are necessary in the operation of the facility.
- C. Employees shall not correspond with or assist in conducting correspondence with inmates, former inmates, or other persons not in custody on behalf of an inmate, unless required to do so in the performance of their duties.
- D. Employees shall not assist inmates in the submission or preparation of judicial documents, other than providing the necessary forms, papers, or writing implements, unless required to do so in the performance of their duties or by court order.
- E. Employees shall not write letters of recommendation on behalf of inmates on matters concerning official business of the Office without authorization from their bureau commander.
- F. Employees shall not exchange money or property with inmates or prisoners, unless required to do so in the performance of their duties.
- G. Employees shall not provide inmates with newspapers, magazines, or books from outside the jail, except those mailed to the inmate from the publisher or that publisher's authorized distributor as governed by Policy DK-1, *Inmate Mail*.
- H. Employees shall not engage in informal, non-work-related discussions with inmates or prisoners concerning other officers, inmates or prisoners. Employees shall not make remarks of a personal nature in reference to any officers, inmates or prisoners, witnesses, or informants where the remarks may be within earshot of any inmate or prisoner.
- I. Employees shall not encourage or sympathize with inmates in their complaints about rules, regulations, or jail conditions. However, complaints will be reported to appropriate personnel.
- J. Employees shall not offer religious or other advice to inmates regarding personal, family, or case-related problems. Inmates seeking advice will be referred to appropriately trained Office personnel or other outside agencies.

19. **Employee Relationships with Persons Visiting Inmates:**

- A. Employees shall not grant special privileges to visitors without the approval of the shift commander.
- B. Employees shall not accept favors or gratuities from visitors at any time.
- C. Employees shall not indulge in undue familiarity or fraternize with visitors.

20. **Employee Relationships with Other Employees:**

- A. Employees shall be respectful and maintain a professional, courteous, and cooperative demeanor with other employees of the Office and other law enforcement or criminal justice personnel.
- B. Employees shall be respectful and maintain a professional, courteous, and cooperative demeanor with supervisory personnel. Employees shall not defy the authority of any supervisor by being disrespectful, arrogant, or displaying disrespectful conduct, whether in or out of the supervisor's presence.
- C. When relatives are employed by the Office, no employee shall be in a reporting line of supervision to a relative. In the event it is determined a relative would be or has been placed in a reporting line of supervision, an appropriate course of action will be determined by the Chief Deputy.
- D. Intimate and sexual relationships between employees are covered in Policy CP-3, *Workplace Professionalism*.
- E. Employees shall not covertly record conversations involving other employees unless the recording is in furtherance of an official department investigation or prior approval for the covert recording has been obtained from a bureau commander or his designee.

21. **Employee Relationships with Known or Suspected Criminals:** Employees shall avoid associations or dealings with persons whom they know or have reason to believe are, or have been, recently charged with criminal acts or are under indictment. Exceptions may be made when necessary in the performance of an employee's duties or when such contacts are with relatives.

22. **Frequenting Prohibited Establishments:** Employees shall not knowingly enter or frequent any establishment, such as a house of prostitution or illegal gambling house, wherein the laws of the United States, the state, or the local jurisdiction are regularly violated, except in the performance of duty or while acting under proper and specific orders from a supervisor.

23. **Gambling:** Employees shall not participate in any form of illegal gambling at any time, except in the performance of duty and while acting under proper and specific orders from a supervisor.

24. **Sleeping On Duty:**

- A. Employees shall not sleep on duty unless specifically authorized to do so.
- B. Employees who feel they are unable to stay awake on duty have the responsibility to notify their immediate supervisor, who shall determine the proper course of action.

25. **Interference with Official Investigations:** Employees shall not use their official position or knowledge gained by employment with this Office to hinder, obstruct, or interfere with any case, official operation, or investigation being handled by this Office or any other agency.

26. **Request for Assistance:** When any person requests assistance from the Office or makes a complaint or report, either by telephone or in person, all pertinent information will be obtained in an official and courteous manner, and will be properly and judiciously acted upon, in accordance with Office Policy.

27. **Failure to Meet Standards:** Failure to meet standards is the inability, unwillingness, or failure to perform assigned duties in an acceptable manner, or the failure to accomplish a reasonable share of the workload. Employees shall:
 - A. Possess the knowledge required to perform assigned duties.
 - B. Complete assignments properly.
 - C. Conform to work standards established for the employee's rank or position.
 - D. Make reasonable decisions or take appropriate actions.
 - E. Not take actions which are unreasonable or clearly inappropriate for the situation.
 - F. Not display cowardice if they are deputies, reserve deputies, or detention officers.
 - G. Not be absent from the assigned area of responsibility during a tour of duty without authorization.
 - H. Not be absent without authorized leave as specified in Policy GC-1, *Compensation, Leaves, and Absences*.
28. **Insubordination:** Insubordination is the willful refusal to obey a reasonable and lawful order. A reasonable and lawful order given to a subordinate shall be followed regardless of the method of conveyance, as governed by Policy GB-2, *Command Responsibility*. The willful failure to obey an order constitutes grounds for discipline, up to and including dismissal from employment.
29. **Loitering:** While on duty or in uniform, employees shall not remain in eating establishments, service stations, or other public places for longer than is reasonably required to complete the legitimate activity for which they stopped, unless required by duty. Employees shall not remain at a duty post or any Office location beyond the end of their shift unless conducting official business or for a minimal period while awaiting transportation from work.
30. **Job Abandonment:** Except when extenuating circumstances are found to have existed, employees shall be considered to have abandoned their position when they have been absent for three or more consecutive working days without authorization. This includes being absent for three or more consecutive working days without authorization following an approved leave of absence.
 - A. On any scheduled workday, if an employee does not have prior authorization or prior supervisory approval and fails to contact their supervisor or the on-duty supervisor prior to the scheduled start time of their shift, the following procedures will be followed:
 1. The supervisor will contact the employee by phone each day to determine if the employee's absence is due to an unexpected emergency. The supervisor will complete a telephone log documenting the time of the call and any information obtained or any messages that were left.
 2. If the supervisor is unable to contact the employee and the employee has not contacted the supervisor for three consecutive workdays, the employee will be deemed to have abandoned their position. The supervisor shall notify their division commander as soon as possible of any employee who has abandoned their position.

- B. When it has been determined that an employee has abandoned their position, an investigation shall be completed, as specified in Policy GH-2, *Internal Investigations*. The completed investigation shall be forwarded through the chain of command to the Compliance Division to ensure due process.
31. **Abuse of Process, Withholding Evidence, and Misappropriation of Property:**
- A. Employees shall not manufacture, conceal, falsify, destroy, remove, tamper with, or withhold evidence or information, or make false accusations in a criminal, traffic matter or administrative matter.
 - B. Employees shall secure all items of evidence in designated property lockers, or other authorized, secured areas, as soon as possible. Employees shall not leave evidence in vehicles, in personal lockers, in or on desks, or in other areas in which it could be subjected to possible tampering or theft. Contraband should also be placed promptly in an appropriate location, pending destruction or other disposition.
 - C. Employees shall not appropriate any County property, evidence, or found or recovered property for their own use.
32. **Treatment of Persons in Custody:** Employees shall not mistreat persons who are in the custody of the Office. Employees shall handle such persons in accordance with established laws and Office procedures. Policy CP-1, *Use of Force*, and ARS §31-101 through §31-146 governs the treatment of persons in custody.
33. **Gum and Tobacco Usage:** Employees in the performance of their duties shall not chew tobacco or gum while making personal contacts with citizens. Further restrictions on tobacco use are specified in Policy GD-4, *Tobacco Products*.
34. **Return of Office and County Property Upon Separation:**
- A. When employees leave the service of the Office, they shall surrender all Office and other County property that was assigned to them while so employed to the Training Division.
 - B. When employees return property damaged through their negligence or deliberate action or fail to return all assigned Office or County property, they may be held criminally or civilly liable.
35. **Property Damage:**
- A. Employees shall immediately notify their supervisor, or if unavailable, the nearest on-duty supervisor, and promptly submit a written report concerning any damage to real or personal property, including vehicles, belonging to the Office, the County, a private citizen, or any other entity or individual, which is a result of, or occurred during, the execution of their official duties or responsibilities.
 - B. Employees shall immediately notify their supervisor and promptly submit a written report concerning any damage to real or personal property, including vehicles, belonging to the Office or the County that occurred while the employee was off duty.
 - C. Employees shall never attempt to work out or negotiate a settlement with any entity or individual regarding personal or County liability when property damage has occurred during the execution of official duties.

36. **Rumors or Gossip:** Employees shall not spread rumors, gossip, or false information which discredits another employee or harms his reputation. Supervisors made aware of violations shall take immediate action to correct the situation and initiate disciplinary action if warranted.

37. **Social Networking Sites:** The use of social networking sites such as Facebook, MySpace, and Twitter have become common outlets for employees to socialize. Employees must be mindful of the negative impact of inappropriate or unauthorized postings involving the Maricopa County Sheriff's Office and their direct impact on the relationship between the Office and the community.

A. Social networking sites shall not be accessed while on duty unless in the performance of official duties.

B. Whether on or off duty, employees shall not publicly express, share, or post information regarding the Office which would jeopardize the safety and security of Office employees, inmates or the public, or which could negatively impact the efficient or effective operation of the Office.

C. Due to the increased scrutiny of law enforcement personnel postings on social networking sites, the Office strongly discourages employees from posting information regarding their own off-duty activities or the off-duty activities of another Office employee which may tend to bring the person's reputation into question. This is not intended to infringe upon any employee's First Amendment or other constitutional rights, but those who may be called to testify on behalf of the Office as part of their official duties must guard their reputation and should be aware that attorneys may attempt to use this type of information, e.g., postings on social networking sites, for impeachment purposes.

38. **Keeping Supervisors Informed:**

A. Employees must promptly notify their supervisors of all situations, events, incidents, inspections, and communications that affect, or may affect, the Office, or with which the Office may be concerned.

B. Examples of situations that require employees to keep their supervisors informed include, but are not limited to, the following:

1. Involvement in any situation being investigated by another law enforcement agency, whether as a witness, victim, or suspect, or in anticipation of becoming a suspect.

2. The suspension or revocation of driving privileges.

3. Receipt of a moving vehicle traffic citation.

4. Knowledge of the booking of a relative into an Office jail.

5. The issuance of a court order, such as an order of protection or an injunction against harassment in which an Office employee has been named.

C. Supervisors should notify their chain of command as appropriate.

39. **Use of Discretion:**

- A. Policy cannot be written to cover every situation in which an employee may become involved. The employee must use discretion in the enforcement of laws and in determining appropriate actions. Supervisors have the authority to make decisions on behalf of the Office and to provide employees with direction and guidance on how to perform their duties.
 - B. When employees are faced with a situation in which discretion can be exercised, they shall evaluate the circumstances and consider available resources and alternate solutions. They should rely on their training, Office Policy, established procedures, statutes, and the direction of supervisors in making a decision.
 - C. The appropriate decision should be the least restrictive one that still accomplishes the intent of the law, is in accordance with Office Policy, and does not compromise employee safety.
 - D. Discretion is limited by federal, state, and local law, as well as case law, Office Policy, and the employee's rank and level of responsibility.
40. **Oath of Office:** The Sheriff or his designee shall administer the Oath of Office to all new sworn and detention personnel prior to assuming their new duties. The Oath of Office requires the employee to support the Constitution of the United States and the Constitution and Laws of the State of Arizona.

EXHIBIT D

JAIL ACCESS POLICY

	MARICOPA COUNTY SHERIFF'S OFFICE	
	Policy & Procedure	Joseph M. Arpaio – Sheriff
	Subject	Policy Number
	JAIL ACCESS	DH-1
		1. Effective Date
		12-10-09
Related Information	Supersedes	
GD-14, <i>Access to Secured Office Buildings</i>	DH-1 (03-28-97)	

PURPOSE

The purpose of this Policy is to identify the various types of authorized jail access cards and passes with which persons are permitted entry into a jail.

POLICY

For the safety of employees, visitors, inmates, the protection of Office property, and the security of criminal justice information, it is the policy of the Office to ensure that entry into the jails is limited by allowing only authorized personnel access.

DEFINITIONS

None

PROCEDURES

1. **Jail Commander Responsibilities:** Jail commanders shall ensure that their jail perimeter is secured so inmates remain within the confines of the jails boundary and access by the general public is restricted.
2. **Authorized Access:** Employees from other agencies, departments, or vendors who perform duties or services not ordinarily completed by Office personnel, may be granted access to jail facilities. Personnel not employed by the Office who may be granted access to a jail include, but are not limited to, the following:
 - A. Emergency services personnel.
 - B. Authorized health care personnel.
 - C. Contract personnel.
 - D. Maricopa County Facilities Management personnel.
 - E. Private vendor personnel.

F. Health and fire inspectors.

3. **Jail Access ID Cards:** Individuals requesting entry into a jail on a regular basis to provide a service or program may be issued Jail Access ID Cards. Upon approval by a custody bureau commander, or his designee, these cards are issued initially for one year and are renewable. Renewals issued subsequent to

the first year will be valid for a period of two years. These issued ID cards allow access to all facilities and will include a photo and an expiration date.

A. After a satisfactory record check, the Custody Support Division may issue the following types of Jail Access ID Cards:

1. The yellow Jail Access ID Card is used by individuals such as inmate programs, religious volunteers, and contracted programs personnel. Yellow card holders are authorized to conduct group meetings or religious services for inmates in areas designated by the jail commander. These card holders are allowed to meet with inmates on a one-on-one basis in visitation, however, are **restricted** from meeting with inmates on a one-on-one basis in inmate housing areas, unless accompanied by a blue card holder.
2. The blue Jail Access ID Card is used by religious advisors, chaplain aides, and contracted chaplains. Blue card holders are authorized to conduct group meetings religious services, and one-on-one meetings with inmates in areas designated by the jail commander.

B. Volunteers and contract personnel with the Custody Support Division, not otherwise employed by the Office who are issued Jail Access ID Cards, must agree in writing to abide by all the rules and regulations contained in the *Custody Support Division Handbook* for volunteers and contract employees. The written agreements will be maintained by the Custody Support Division Commander or his designee.

C. Individuals possessing an expired or revoked Jail Access ID Card shall not be permitted entry into the jail. Detention personnel will confiscate the expired or revoked card and forward it through the chain of command, along with a memorandum, to the Custody Support Division Commander. The memorandum will include details of the confiscation and any other actions taken. Questions regarding this action will be referred to the Custody Support Division Commander, or his designee, through the chain of command.

4. **Visitor Pass Cards:** Visitor Pass Cards are issued to individuals requesting intermittent or temporary access into a jail to provide a service or program. These access cards do not contain a photograph of the individual but are temporarily exchanged for personal ID. Prior approval by the jail commander, or his designee, may also be required. The individual will be instructed to display the Visitor Pass Card on the outer garment so that it will be readily seen at all times while the visitor is inside the jail.

A. The Visitor Pass Card may be used by individuals including, but not limited to, the following:

1. News media personnel.
2. Officers of the court.
3. Contractor vending company employees.

4. Volunteers for inmate programs and religious services.
 5. Jail tour participants.
 6. Private physicians or other qualified medical personnel requested by an inmate to obtain blood or urine samples.
 7. Employees of other law enforcement or correctional agencies who are in civilian attire.
 8. Temporary medical personnel employed by contracted health services.
- B. Individuals requesting a Visitor Pass Card must provide proper ID and proof of profession, or must have been pre-approved by the jail commander, prior to being allowed entry into the jail. Valid forms of ID are specified in Policy DK-3, *Inmate Visitation*.
 - C. The names and dates of birth of all visitors to whom Visitor Pass Cards have been issued will be documented in the Visitation Logbook.
 - D. At least annually, each jail commander shall be responsible for redesigning and printing new Visitor Pass Cards and ensuring that the old cards have been accounted for and destroyed.
5. **Courtesy ID Cards:** Contractors and vendors that work with the Information and Technology Bureau will be issued Courtesy ID Cards after a satisfactory record check is completed by the Personnel Services Division. Courtesy ID Cards will include a photo and an expiration date and will be issued as followed:
 - A. Red Stripe ID: Persons displaying this ID shall be granted access to all Office facilities, including the jails.
 - B. Blue Stripe ID: Persons displaying this ID shall be granted access to all Office facilities, excluding the jails.
6. **Correctional Health Services (CHS) Blue Framed ID:** A blue frame ID shall be issued by CHS, as a Courtesy to CHS personnel. This ID shall be carried with their Maricopa County Employee ID.
7. **Office Personnel Identification:** All Office personnel, uniformed or non-uniformed, shall display their ID upon entering a jail facility. Non-uniformed personnel shall continue to visibly display their ID on their clothing while inside the building.
 8. **Citizen Observer Cards:** Citizen Observer Cards are issued to individuals who accompany sworn personnel on routine patrol duties. The card, which does not contain a photograph, shall be displayed on the observer's outer garment at all times while in a jail.
 9. **Non-Uniformed Officers of other Law Enforcement Agencies:** A non-uniformed officer representing another law enforcement agency will be required to present his agency's ID card prior to entering a jail. However, he will not be required to surrender it. Prior to admission into the jail, the officer will be required to inform detention personnel of his purpose. When his identity has been confirmed, the officer may enter the jail displaying his agency ID card, badge, or Visitor Pass Card. Detention personnel will ensure that all ammunition, knives, and all firearms, including concealed firearms, are secured in a gun locker.

10. **Former Employees:** Former employees of the Office will not be allowed entry into a jail unless they have received prior approval by the jail commander, are presently employed with a law enforcement agency, representing a community related organization authorized to perform a service or program for the Office, or visiting an inmate.
11. **Emergency Situations:** In emergency situations, emergency response personnel such as police officers, fire fighters, or paramedics do not need to be issued a Jail Access ID Card or a Visitor's Pass Card. However, they will be escorted by detention personnel whenever feasible.
12. **Visitor Records Check and Search:** All persons other than law enforcement personnel requesting access into a jail are subject to an Arizona Crime Information Center/National Crime Information Center

ACIC/NCIC check and a search of their person and possessions for possible contraband. Procedures for dealing with those who fail these checks are specified in Policy DK-3, *Inmate Visitation*.

13. **Revoked Access Privilege:** A custody bureau commander may revoke an individual's access privilege by notifying the Custody Support Division Commander. He shall ensure that the issued ID card has been retrieved and, when necessary, shall send written notification to each jail listing the name of the individual whose card has been revoked. Reasons for revocation include, but are not limited to, the following:
 - A. Failure to observe Office or jail rules and regulations.
 - B. Failure to conduct job functions in a reasonable and professional manner.
 - C. Actions or behaviors which threaten the safety or security of a jail.
 - D. Serious violations of a local, State, or Federal law.

EXHIBIT E

INMATE VISITATION POLICY

	MARICOPA COUNTY SHERIFF'S OFFICE	
	Policy & Procedure	Joseph M. Arpaio – Sheriff
	Subject INMATE VISITATION	Policy Number DK-3 1. Effective Date 02-16-11
Related Information DH-1, <i>Jail Access</i>	Supersedes DK-3 (09-19-08)	

PURPOSE

The purpose of this Policy is to establish guidelines for authorizing inmate visitation.

POLICY

The Office recognizes the importance of inmates being able to receive visits from clergy, family, legal counsel, and others to enable them to maintain family and community ties whenever possible. It is the policy of the Office to provide for visitation as safety and operational concerns allow.

DEFINITIONS

Authorized Community Clergy: Lay or ordained ministers from a religious organization who are authorized for Privileged Visits upon approval by Religious Services. A notation is placed by a chaplain in the Jail Management System (JMS) after the citizen's identity is checked, his clergy status confirmed, and the chain of command approves the Privileged Visit. A letter of sponsorship is retained in a personnel file by Religious Services.

Chaplain's Aide or Religious Advisor: A religious volunteer selected for specific duties by, and working directly under the supervision of, staff chaplains. A chaplain's aide or religious advisor is afforded the same considerations as a staff chaplain, including access to housing areas in designated facilities.

Community Clergy: Lay or ordained ministers from a religious organization who are authorized for a visit with an inmate who have not been pre-authorized by Religious Services. The visit will normally be treated as a Special Visit.

Letter of Introduction for Legal Privileged Visitor Status: A form letter which, when presented with valid photo identification qualifies legal personnel for Privileged Visitor Status. Each form letter must be an original, fully completed and signed by attorney of record at the time of the visit, if the attorney of record is not present at the time of the visit, the original form letter must be presented as an attachment to a signed original letter on official letterhead that includes a street address and business phone number of the legal organization sponsoring the visitor. The person signing the letter may or may not be the visitor. The letter states the name of the visitor, name of the inmate, the inmate's booking number, and the purpose of the visit. A separate letter is required for each inmate to be visited and must be presented for each visit. Each letter is valid for 60 days after its original issuance.

Letter of Introduction for Special Visitor Status: A form letter which, when presented with valid photo identification qualifies community clergy for Special Visitor Status. Each form letter must be an original, fully completed and signed by a religious official. The original form letter must include a street address and business phone number of the religious organization sponsoring the visitor. The person signing the letter may or may not be the visitor. The letter states the name of the visitor, name of the inmate, the inmate's booking number, and the purpose of the visit. A separate letter is required for each inmate to be visited and must be presented for each visit. Each letter is valid for 60 days after its original issuance.

Officers of the Court: Professionals who are authorized to have Privileged Visits with inmates. They include, but are not limited to, the following:

1. Attorneys and probation officers.
2. Legal assistants, paralegals, mitigation specialists, and investigators with valid Maricopa County employee identification.
3. Private investigators with a valid private investigator license and a *Letter of Introduction for Legal Privileged Visitor Status*.
4. Doctors, psychiatrists, or psychologists, and counselors with current Maricopa County employee identification.
5. Court reporters, paralegals, and legal assistants from private law firms, and court-appointed interpreters when accompanied by an attorney.

Staff Chaplain: A religious representative employed or contracted by the Office.

Visitation Categories: Categories of visitation used by the Office. Visits may be recorded except for visits with Officers of the Court which require a Court Order to record.

1. **Regular:** A visit made by an individual who resides within Maricopa County. Visits by friends and family members are Regular Visits unless otherwise authorized by the jail commander or his designee. Inmates are allowed to have three 30-minute, Regular Visits in a seven-day period.
2. **Out-of-County:** A visit made by an individual who resides outside of Maricopa County. Inmates are allowed to have three 30-minute, Out-of-County Visits in a seven-day period. Out-of-County Visits do not count against other categories of inmate visits. Additional visits for individuals traveling from out-of-state may be granted within a seven-day period at the discretion of the jail commander or his designee. These visits will only be allowed during regularly scheduled visitation hours, unless otherwise approved by the jail commander or his designee.
3. **Privileged:** A visit made by Officers of the Court, a consular or embassy officer, chaplain's aide, religious advisor, community clergy or authorized community clergy. Privileged Visits are normally Contact Visits, regardless of the inmate's classification. They are normally conducted in the visitation area during regularly scheduled visitation hours and have no set time limit unless limitation is required for the secure and orderly operation of the jail. The visit does not count against the other categories of inmate visits. Prior to the visit, the visitor's status must be confirmed by proof of professional status or JMS confirmation, along with valid photo identification. Proof of professional status may be established by an Arizona Bar Association Card, a listing of contract providers supplied by the superior court, a *Letter of Introduction* or through a notation in JMS made by Religious Services. If the visitor is not able to provide proof of profession or is a

relative of the inmate, but does possess valid identification, he may be allowed a Regular Visit.

4. **Special:** A visit that is designated for community clergy or police officers. Special Visits have the same requirements as Regular Visits. Special Visits for community clergy may be authorized by the jail commander, his designee, or a staff chaplain. The approval must be verified in writing along with a *Letter of Introduction for Special Visitor Status*. Special Visits may be Video, Contact, or Non-Contact in accordance with the inmate's security level, conducted in the visitation area, and have no set time limit; they must occur during regular visitation hours unless limitation is required for the secure and orderly operation of the jail. The visit does not count against the other categories of inmate visits. If unable to provide the required documentation, the visitor may be allowed to have a Regular Visit, as specified in this Policy. These visits will not entitle an in-custody inmate to be called upon for translation.
 - a. Paralegals or legal assistants requesting a Special Visit with a member of their immediate family or a pro per inmate shall require the approval of the jail commander or his designee. Prior to granting the visit, the visitor will be required to present a *Letter of Introduction for Special Visitor Status*, along with a valid form of identification.
 - b. A pro per inmate must have prior approval from the jail commander, or his designee, prior to being granted a Special Visit with witnesses. In all cases, the visits shall be Non-Contact.
5. **Courtesy:** A visit that may be given at the discretion of the jail commander or his designee. This classification may be used for visits that do not fall into the other categories of visits. Courtesy Visits may be Video, Contact, or Non-Contact in accordance with the inmate's security level, conducted in the visitation area, and have no set time limit unless limitation is required for the secure and orderly operation of the jail. This visit does not count against the other categories of inmate visits.
 - a. A person requesting a Courtesy Visit with a member of his immediate family will be required to obtain the approval of the jail commander, or his designee, prior to being granted the visit. The visit may be used for such matters to include, but not be limited to, death notification by the family member or out-of-state visits that have unique circumstances. If the Courtesy Visit is not approved, the visitor may be allowed to have a Regular Visit, as specified in this Policy.
 - b. Bondsmen will be given Courtesy Visits. They must follow the Special Visit guidelines at jails with visitation. At jails without visitation, prior approval by the jail commander, or his designee, may be required to obtain a Visitor Pass Card. This will permit entry into specified areas for conducting official business only, as specified in Policy DH-1, *Jail Access*. If the bondsmen are unable to provide the required documentation, they may be allowed to have a Regular Visit, as specified in this Policy.

Visitation Types: Visitation methods used by the Office in order to ensure the visitation process is safe for inmates, staff, and visitors, and does not interfere with the security and operation of the jail.

1. **Contact:** A visit that authorizes limited physical contact between inmates and their visitors. Medium and minimum-security inmates are allowed Contact Visits unless otherwise restricted by security, disciplinary, or medical reasons. Maximum security and

closed custody inmates are allowed Contact Visitation for Privileged Visits only, unless prohibited by the jail or shift commander.

2. Non-Contact: A visit that allows oral communication and visual contact between the inmate and the visitor, but prohibits any physical contact between them. The inmate and visitor are usually separated by a transparent partition. Maximum security and closed custody inmates are allowed Non-Contact Visitation, unless otherwise specified by Policy, or restricted for security, disciplinary, or medical reasons.
3. Video: Inmate access to the Video Visitation System for Video Visits is provided at the Tents facility, Lower Buckeye Jail, and the 4th Avenue Jail. Video Visits may be used for all Visitation Categories.

PROCEDURES

1. **General Procedures:** Each jail shall provide an area which allows communication between inmates and their visitors, but does not jeopardize the security and operation of the jail.
 - A. Individuals categorized as Regular or Out-of-County visitors will not be allowed to visit under more than one category in any 30-day period. As space permits, an Out-of-County or Regular Visit may be extended by using consecutive visits, which shall be deducted from the number of visits remaining in that seven-day period.
 - B. Visitors may only visit one inmate at a time regardless of the type of visit. Inmates will be restricted to a maximum of two visitors per visit, excluding Privileged Visits. Two visitors at the same time will be counted as one visit when computing the number of remaining visits for the inmate.
 - C. Barring unusual circumstances, the jail commander will ensure that visitation procedures provide for a Privileged Visit to begin within 15 minutes of the request.
 - D. Prior approval must be granted by the jail commander before a Privileged Visitor is allowed to bring in specialized equipment, such as video or photographic equipment. Tape recorders may be allowed with the visitation supervisor's approval; however, they may only be used in the visitation area.
 - E. During a Privileged Visit, a high-risk inmate may be allowed to visit in a secured, non-partitioned area, separate from other visitors, thus permitting confidential communication between the inmate and the visitor. Security devices may be applied to the inmate to ensure the security of the jail and the safety of the visitor.
 - F. Religious Services shall screen and approve all Privileged Visits for chaplain's aides or religious advisors, and authorized community clergy.
 1. Upon approval by a staff chaplain, chaplain's aides, religious advisors, and contracted chaplains will be given a blue Jail Access Identification Card, as specified in Policy DH-1, *Jail Access*.
 2. Upon approving Privileged Visits for authorized community clergy, Religious Services will make a notation in JMS, authorizing a Privileged Visit between the indicated clergy and the inmate. Upon requesting a Privileged Visit, visitation staff shall ask for a valid photo ID and access JMS to confirm the privileged status of the visit; possession of a *Letter of Introduction* is not needed at the time

of the visit. Religious Services staff shall control the number of inmates with whom a clergyman has requested Privileged Visitor Status.

2. **Inmates in Segregation:** Inmates in segregation may be allowed to receive visitors; however, special conditions or limitations may be placed on their visitation privileges.
 - A. Inmates in administrative segregation housing are allowed visitation privileges unless there are significant security reasons to deny the visit or disciplinary sanctions have been imposed which specifically warrant denying visitation. Privileged Visits may still be allowed.
 - B. Inmates suspected of having a serious, casually transmitted, communicable disease, as specified in Policy CP-6, *Bloodborne Pathogens* or CP-7, *Airborne Pathogens*, may be denied visitation privileges. Privileged Visits may be allowed upon approval of a Correctional Health Services (CHS) provider.
3. **Persons Requesting a Visit:** Persons requesting a visit with an inmate must provide a valid photo ID. Each visitor's identification information will be recorded in JMS.
 - A. An Arizona Crime Information Center (ACIC) and National Crime Information Center (NCIC) warrant check will be conducted on the visitor.
 1. If a warrant is found, the supervisor will be notified immediately.
 2. Operations Information Center (OIC) or the Originating Agency (ORI), if within the State of Arizona, shall be contacted to confirm the warrant.
 3. If the warrant is valid and the visitor is believed to be the individual named in the warrant, the supervisor will be advised, and he shall request that a sworn officer be dispatched to make the arrest.
 4. The visitor shall be allowed to have a visit, pending his arrest by sworn personnel. If the visitor concludes his visit prior to the arrival of a sworn officer, non-sworn personnel shall not physically detain the visitor based solely upon the warrant. However, delaying tactics such as extending visit limits or asking to reconfirm visitor identification are appropriate, particularly in felony cases, as long as the visitor has not asked for or been refused exit from the jail.
 - B. Minors under the age of 18 must be accompanied and supervised by an adult during a visit.
 1. Minors under one year of age are not counted as visitors. Minors 1 through 17 years of age are considered visitors.
 2. Minors under the age of 14 shall not be required to provide identification unless their age or identity is in question.
 3. Any minor between the ages of 14 and 17 shall be required to present a current ID, such as a school ID card.
 4. A minor who is married to an inmate must provide a marriage certificate and valid identification. The married minor is not required to be accompanied or supervised by an adult.

- C. Persons requesting a Regular or Out-of-County Visit will be required to declare their citizenship status. Non-citizens are required to provide information regarding their legal status.
4. **Valid Identification:** For identification to be considered valid, it must be issued to the bearer, be current, and contain at a minimum, a picture of the visitor and the visitor's name, sex, and date of birth. Personal identification not indicating a current address must be substantiated with other forms of identification or current, postmarked mail with the individual's name and address on the envelope. The following are valid types of identification approved for visitation and jail access purposes; no other types of identification are acceptable unless authorized by the supervisor or jail commander:
 - A. Federal, State, and local government-issued identification cards.
 - B. State-issued driver's licenses.
 - C. Arizona Bar Association Cards in conjunction with another form of acceptable identification.
 - D. Court orders in conjunction with another form of acceptable identification.
 - E. Letters of Introduction, in conjunction with another form of acceptable identification.
 - F. High school identification cards if the visitor is under the age of 18 and does not possess any other valid identification
 - G. Social Service Cards with the bearer's photograph issued by the Arizona Department of Economic Security.
 5. **Subject to Search:** All visitors are subject to a search prior to, during, or after a visit with an inmate. All visitors regardless of age must, at a minimum, pass through an electronic metal detector, if available, or be searched with a hand-held metal detector prior to entering the visitation area. Refusal to be searched will automatically cause the visit to be canceled and all future visits to be denied. A memorandum will be completed and forwarded through the chain of command to the appropriate custody bureau commander and the individual's name will be added to a list of prohibited visitors.
 6. **Visitors Storage of Personal Property:** A locker or secured area will be provided for visitors to store personal property at their own risk. Personal property which is not allowed in the visitation area includes, but is not limited to, purses, cigarettes, wallets, jewelry, and money.
 7. **Contraband:** Procedures regarding contraband found during a visit are specified in Policy DH-3, *Contraband Control*.
 8. **Visitation Dress Code:** The visitation dress code will be enforced prior to and throughout the visit. Questions concerning appropriate dress shall be referred to a supervisor to determine whether the visit will be permitted. Dress code violations include, but are not limited to, the following:
 - A. Wearing swimming attire.
 - B. Wearing clothing which is above mid-thigh, to include cutoffs, shorts, dresses, and skirts.
 - C. Wearing see-through clothing, including, but not limited to, sheer blouses or any other clothing considered to be revealing.

- D. Not wearing a shirt, or wearing clothes which make the breasts visible.
 - E. Wearing clothing, such as a tube top, tank top, or halter top which exposes excessive cleavage, the midriff, or the shoulders, irrespective of the visitor's gender.
 - F. Having bare feet.
 - G. Wearing or displaying clothing or paraphernalia which identifies a specific gang by name or logo.
 - H. Any visible gang related tattoos.
9. **Visitation after Incarceration:** Individuals who have been incarcerated in any correctional, detention, or booking facility, regardless of the duration of time spent in custody, including those who have been processed on a summons booking, shall be required to wait for a period of one year from the date of their release prior to being granted a visit with any inmate. Visitors who wish to be exempted from this one-year requirement shall be required to present a written request to the respective division commander for approval. If approved, the exemption shall be noted in JMS.
10. **Prohibited Visitors:** If it is determined that an individual is on parole, probation, any type of work release, or has ever been convicted of a felony, he may not enter or be approved for visits within any Office jail.
11. **Visitation Hours:** Visitation may only be conducted on designated days and hours, as determined by command staff. Jails may also discontinue visitation for scheduled periods during meals or as necessary for the security and safety of the jail.
12. **Designated Visitation Areas:** Visits will take place only in designated visitation areas and will not be conducted in inmate living areas.
13. **Termination or Suspension of a Visit:** A visit may be terminated or suspended by a supervisor or the jail commander. The supervisor may also request that the visit not be charged to the inmate and that the appropriate deletion be made in JMS. Reasons for terminating or suspension of a visit include, but are not limited to, the following:
- A. The existence of disciplinary or medical restrictions.
 - B. The visitor appears to be under the influence of alcohol or drugs.
 - C. The visitor is refusing to submit to search procedures, as specified in this Policy.
 - D. The visitor is refusing to provide proper identification, as specified in this Policy, or has provided false identification.
 - E. The visitor is violating the visitation dress code.
 - F. The visitor and inmate are engaging in any physical contact, including, but not limited to, fondling or fighting.
 - G. The visitor is disrupting other visitors.
 - H. The visitor or inmate is violating jail rules.

- I. The security of the jail requires it.
 - J. There is insufficient visitation space.
 - K. Children are not properly supervised or are left unattended during the visit.
14. **Strip Search:** All inmates concluding a contact visit will be strip searched prior to being returned to their housing units.

**ADDENDUM A
SUMMARY OF CLERGY VISITATION**

PRIVILEGED VISITS

- 1. Must pass through metal detectors for entry into jail. Unless a security concern, does not have to secure personal items.
- 2. All items brought into the jail must be inspected either electronically or manually.
- 3. Clergy materials permitted for visit include, but are not limited to, the following:
 - A. Bible, Koran, Book of Mormon, electronic Bibles, and other religious texts.
 - B. Prayer books, pamphlets, religious magazines, and scripture study material.
 - C. Items used for religious services such as, bread, oils, or Native American smudge.
- 4. Religious materials for the inmate may be left with the permission of the Visitation officer and in accordance with the Rules and Regulations for Inmates.
- 5. A Contact Visit is permitted except, as specified in this Policy.
- 6. Visitation hours are according to the inmate's classification, as posted. Visits for other than posted hours will require the authorization of the jail commander or his designee.

SPECIAL VISITS

- 1. Must pass through metal detectors for entry into jail. Must secure all personal items in visitor locker.
- 2. All items brought into the jail must be inspected either electronically or manually.
- 3. Clergy materials permitted for visit, include, but are not limited to, the following:
 - A. Bible, Koran, Book of Mormon, electronic Bibles, and other religious texts.
 - B. Prayer books, pamphlets, religious magazines, and scripture study material may be left at the Visitation desk for the inmate in accordance with Rules and Regulations for Inmates.
- 4. Other religious items will not be brought into the jail unless prior permission has been obtained by the jail commander or his designee.

5. A Contact Visit is not authorized for an inmate who has been classified as Non-Contact or for security or health reasons, as specified in this Policy.
6. Visitation hours are according to the inmate's classification, as posted. Visits for other than posted hours will require the authorization of the jail commander or his designee.

EXHIBIT F

CURRENT VIDEO VISITATION SYSTEM EQUIPMENT

4th Ave:

Item	Description	Qty.
Audio/Video Switch	Video Switch Duplex	1
	Audio Switch Duplex	
System Server	IBM Server	1
MTISW	VVS Scheduling Software	
Visitation Stations (cell blocks)	Audio/Video Terminals	113 Units
	1/4" CCD Board Cameras -Samsung SCC-B1311	
	15" LCD Monitors-Planar 1503RLCD	
Visitation Stations (lobby)	14" Monitors-Samsung SMC145 crt	38 Units
Isolation Terminals	Rollabouts	16 Units
Wire Encoders/Decoders	Wire Amps	212 Units

4th Ave Remote Access Video Visitation:

Item	Qty.
Polycom VS4000	16
ADA Booths	1
Non-ADA Booths	5
Shelving units for VS4000	16
Interconnecting patch panel	1

Hardware:

AV Talon Triplex Multiplexer – Model Talon4
 Ultrak HD Series Max-1000 CCTV Management System – Model MX32128
 Ultrak Maxpro System Contoller - Kegs5300
 Ultrak Mxat200 System Controller
 Ultrak Max-1000 MX18 Expander
 Ultrak Max-1000 MXPS9 System power supply
 NVT (Network Video Technologies) NV-3213A CCTV Twisted Pair Passive Transceiver Hub
 Ultrak MXBNC128
 IBM X Series 345 Server
 Honeywell ENT DVR – ES A16U-61410
 ENC 8M2\AFRR (Alpha Frame Rate Production)
 Fast Power supply
 Netgear Switch
 Micro Comm DXI – Model # SAC-110-155-313 Harding Instrument
 ABSOPULSE Electronics LTP
 DXI ACB Board Harding Instrument
 DXI ATB Board Harding Instrument
 DXI SAB Board Harding Instrument
 DXI AOB Board Harding Instrument
 Mobile Black Racks
 UPS 750 APC
 Planer PT 170M Touchscreen
 Compaq Presario SR1120NX
 Hp Laser Jet 1012

Software:

Windows 2000 Professional
 Windows XP

Lower Buckeye Jail

Item	Description	Qty.
Audio/Video Switch	Video Switch Duplex	1
	Audio Switch Duplex	
System Server	IBM Server	1
MTISW	VVS Scheduling Software	
Visitation Stations (cell blocks)	Audio/Video Terminals	110 Units
	1/4" CCD Board Cameras -Samsung SCC-B1311	
	15" LCD Monitors-Planar 1503RLCD	
Visitation Stations (lobby)	14" Monitors-Samsung SMC145 crt63	Units
Conference/Medical Terminals	Rollabouts	12 Units
Wire Encoders/Decoders	Wire Amps	206 Units

Lower Buckeye Jail, Remote Access Video Visitation:

Item	Qty.
Polycom VS4000	16
ADA Booths	2
Non-ADA Booths	5
Shelving units for VS4000	16
Interconnecting patch panel	1

Estrella Support Building:

Item	Description	Qty.
Audio/Video Switch	Video Switch Duplex	1
	Audio Switch Duplex	
System Server	IBM Server	1
MTISW	VVS Scheduling Software	
Visitation Stations (cell blocks)	Audio/Video Terminals	61 Units
	1/4" CCD Board Cameras	
	15" LCD Monitors-Planar 1503RLCD	

MMC Ward 41:

1	15"LCD Monitor
1	20" CRT Monitor
2	Color Camera
2	Lens
4	Handsets

EXHIBIT G**POD CAPACITY LISTING**

Facility	House	Pod	Capacity
4 th Ave	2A	100	120
4 th Ave	2A	200	72
4 th Ave	2B	100	72
4 th Ave	2B	200	72
4 th Ave	2C	100	72
4 th Ave	2C	200	72
4 th Ave	2D	100	72
4 th Ave	2D	200	72
4 th Ave	2E	100	72
4 th Ave	2E	200	72
4 th Ave	2F	100	36
4 th Ave	2F	200	36
		LEVEL TOTAL	840
4 th Ave	3A	100	72
4 th Ave	3A	200	72
4 th Ave	3B	100	72
4 th Ave	3B	200	72
4 th Ave	3C	100	72
4 th Ave	3C	200	72
4 th Ave	3D	100	72
4 th Ave	3D	200	72
4 th Ave	3E	100	72
4 th Ave	3E	200	72
4 th Ave	3F	100	72
4 th Ave	3F	200	72
		LEVEL TOTAL	864
4 th Ave	4A	100	36
4 th Ave	4A	200	36
4 th Ave	4B *	100	18*
4 th Ave	4B *	200	18*
4 th Ave	4B *	300	18*
4 th Ave	4B *	400	18*
4 th Ave	4E *	100	18*
4 th Ave	4E *	200	18*
4 th Ave	4E *	300	18*
4 th Ave	4E *	400	18*
4 th Ave	4F	100	36
4 th Ave	4F	200	36
4 th Ave	SMU1 *	1	18*
4 th Ave	SMU2 *	2	18*
4 th Ave	SMU3 *	3	18*
4 th Ave	SMU4 *	4	18*

* Denotes the use	of portable roll-a-bouts	LEVEL TOTAL	360
		Facility Totals:	2064
Facility	House	Pod	Capacity
LBJ	T11	A	72
LBJ	T11	B	70
LBJ	T12	A	72
LBJ	T12	B	70
LBJ	T13	A	72
LBJ	T13	B	70
LBJ	T14	A	72
LBJ	T14	B	70
		LEVEL TOTAL	568
LBJ	T21	A	72
LBJ	T21	B	70
LBJ	T22	A	72
LBJ	T22	B	70
LBJ	T23	A	72
LBJ	T23	B	70
LBJ	T24	A	72
LBJ	T24	B	70
		LEVEL TOTAL	568
LBJ	T31	A	72
LBJ	T31	B	70
LBJ	T32	A	72
LBJ	T32	B	70
LBJ	T33	A	72
LBJ	T33	B	70
LBJ	T34	A	72
LBJ	T34	B	70
		LEVEL TOTAL	568
LBJ	M1	-	102
LBJ	M2	-	102
LBJ	M3	-	102
LBJ	M4	-	102
		LEVEL TOTAL	408
LBJ	P1	A	15
LBJ	P1	B	15
LBJ	P2	A	18
LBJ	P2	B	18
LBJ	P3	A	18
LBJ	P3	B	18
LBJ	P4	A	18
LBJ	P4	B	18
LBJ	P5	A	18
LBJ	P5	B	18
LBJ	P6	A	18

LBJ	P6	B	18
		LEVEL TOTAL	210
Facility	House	Pod	Capacity
LBJ	Infirmary *	-	60*
		Facility Totals:	2382
Facility	House	Pod	Capacity
Durango	D1	A	64
Durango	D1	B	64
Durango	D1	C	64
Durango	D1	D	64
Durango	D2	A	64
Durango	D2	B	64
Durango	D2	C	32
Durango	D2	D	64
Durango	D3	A	31
Durango	D3	B	64
Durango	D3	C	64
Durango	D3	D	64
Durango	D4	A	64
Durango	D4	B	64
Durango	D4	C	64
Durango	D4	D	64
Durango	D5	A	64
Durango	D5	B	64
Durango	D5	C	64
Durango	D5	D	64
Durango	D6	A	64
Durango	D6	B	64
Durango	D6	C	64
Durango	D6	D	64
Durango	D7	A	64
Durango	D7	B	64
Durango	D7	C	64
Durango	D7	D	64
Durango	D8	DORM	258
Durango	D9	DORM	258
		Facility Totals:	2243
Facility	House	Pod	Capacity
Towers	T1	A	30/45
Towers	T1	B	30/45
Towers	T1	C	30/45
Towers	T1	D	30/45
Towers	T2	A	30/45
Towers	T2	B	30/45
Towers	T2	C	30/45
Towers	T2	D	30/45
Towers	T3	A	30/45

Towers	T3	B	30/45
Towers	T3	C	30/45
Towers	T3	D	30/45
Towers	T4	A	30/45
Towers	T4	B	30/45
Towers	T4	C	30/45
Towers	T4	D	30/45
Towers	T5	A	30/45
Towers	T5	B	30/45
Towers	T5	C	30/45
Towers	T5	D	30/45
Towers	T6	A	30/45
Towers	T6	B	30/45
Towers	T6	C	30/45
Towers	T6	D	30/45
30/45	30= NORMAL 45= OVERFLOW	Facility Totals:	720/1080
Facility	House	Pod	Capacity
Estrella	A	100	30
Estrella	A	200	30
Estrella	A	300	30
Estrella	A	400	30
Estrella	B	100	30
Estrella	B	200	30
Estrella	B	300	30
Estrella	B	400	30
Estrella	C	100	30
Estrella	C	200	30
Estrella	C	300	30
Estrella	C	400	30
Estrella	D	100	30
Estrella	D	200	30
Estrella	D	300	30
Estrella	D	400	30
Estrella	M	100	14
Estrella	M	200	14
Estrella	E	DORM	128
Estrella	F	DORM	128
Estrella	G	DORM	128
Estrella	I	DORM	102
Estrella	J	DORM	128
Estrella	K	DORM	130
Estrella	L	DORM	128
		Facility Totals:	1380
Facility	House	Pod	Capacity
Tents	N	Tents N Yard	568

Tents	O	Tents O Yard	240
Tents	H	Tents Yard 1	352
		Facility Totals:	1160

EXHIBIT H

MCSO SECURITY GUIDELINES

PART 1 – GENERAL ACCESS REQUIREMENTS AND SECURITY BACKGROUND CHECKS

For the purpose of this procedure, the following terms shall apply

Acceptable ID: Identification documents such as a driver's license, passport or military ID which contain at a minimum: date of birth, sex and either a clear photograph or a second numerical identifier, such as a Social Security number. If an Arizona Driver License number is not submitted, the applicant must submit a digital photograph that will be used during the background investigation and for an ID card if appropriate.

Contractor Personnel: Non-employees who provide services in any Sheriff's Facility on a regular or irregular basis. Contractor personnel shall have entry to detention or district facilities at the discretion of the Sheriff or his designee for the duration of the construction project.

Contractor personnel shall complete a Sheriff's Office Application For Courtesy Identification prior to performing any services, or gaining access to any Sheriff's Office Facility. Application forms shall be completely and legibly filled out and signed. False statements shall be grounds for disqualifying the applicant. Application forms shall be submitted to the Facilities Management Project Manager who will then forward the forms to the Sheriff's Office Facilities Project Coordinators for processing. Forms must be submitted to the Maricopa County Sheriff's Office Facilities Project Coordinators in the Construction Maintenance Division at least TEN (10) working days prior to the date required to access the facility. You can reach Karl Gosch at 602-876-4479 or by cell at 602-527-2194 (Tues – Fri). You can also reach Charles Grimes at 602-876-1896 or by cell at 602-527-5714 (Mon –Thur).

The information provided on the Maricopa County Sheriff's Office Application for Courtesy Identification form will be used to conduct a criminal history check. Any resulting criminal history documentation will be forwarded to the Sheriff's Office Facilities Project Coordinator, or his designee. It will be reviewed on a case by case basis to determine whether the applicant poses any risk to the safety of any persons, or to the security of any jail or facility.

Applicants must meet the following conditions to be approved by the Sheriff or his designee for access to Sheriff's Office Facilities:

- a. Be at least eighteen (18) years of age. There will be no exceptions.
- b. At least twelve (12) months must have elapsed since serving a term of probation or parole.
- c. If the ex-offender served a jail sentence as the result of a misdemeanor conviction, a minimum of twelve (12) months must have elapsed since last being incarcerated in any jurisdiction.
- d. If the ex-offender served a jail or prison term as a result of a felony conviction, access will be denied.

Contractor personnel who are approved after a criminal history check shall be issued a Sheriff's Office Facility Visitor Card. The card remains the property of the Sheriff's Office and may be revoked if the following rules and regulations are not adhered to:

- a. The card shall be worn in plain view on the front of the shirt or on a chain around the neck at all times while in a Sheriff's Office facility.
- b. All personnel are required to submit to a search for contraband, if asked.
- c. Contractor personnel are prohibited from duplicating the card.
- d. Contractor personnel who lose their access cards shall report the loss to the Jail Commander or Sheriff's Office Facilities Project Coordinator as soon as possible.
- e. Allowing another person to use the I.D. Card is prohibited.

Contractor personnel who are approved after a criminal history check may be placed on a list and only those listed will have access to the Sheriff's Office Facility or Grounds.

Contractor's personnel who become involved in a criminal investigation during the contract period, either on the job or on their own time, must notify the Sheriff's Office Facility Planning Coordinator within twenty-four hours. Contractor's personnel access may be subsequently suspended or revoked at the discretion of the Sheriff's office Facility Planning Coordinator, Facility Commander/ District Commander or designee.

All concerns regarding contractor personnel should be forwarded to the Sheriff's Office Facility Planning Coordinator. The services of any contractor may be reduced, postponed or discontinued for any of the following reasons:

- a. Violating these guidelines.
- b. Participating in unlawful or immoral conduct.
- c. Showing signs of an illness or condition that might interfere with the individual's ability to perform his duties or threaten the security, health or safety of any one involved.
- d. Reporting to work with any odor of intoxicating beverage on their breath or while under the influence of any intoxicating beverage to any degree.
- e. Behaving in a manner which threatens the safety and security of the jail, staff or inmate.
- f. Unauthorized contact with inmates.
- g. Possession or use of any controlled substances, narcotics or hallucinogens, except when prescribed by a physician, for any illness or injury unless otherwise provided by the Arizona Revised Statutes.
- h. Possession of any weapon on or near County property.
- i. Failure to follow the directions of a Sheriff's Office Staff.
- j. Being in an unauthorized area.
- k. Possession of tobacco products, alcohol, and weapons are strictly prohibited on jail premises.
- l. Under no circumstances will cell phone cameras be used without the express permission of the Jail Commander/District Commander or designee.
- m. Under no circumstances will MP3 players, radios, I-Pods or similar devices be permitted on to the facility.

The Sheriff's Office Facility Visitor Card is to be used for no other purpose than to access the specific areas related to the project in progress. On completion of the project, the cardholder shall immediately return the card to the Jail Commander/District Commander, or the Sheriff's Office Facility Planning Coordinator.

PART 2 – FACILITY ENTRY AND EXIT REQUIREMENTS

Entry into and exit from the job site will be coordinated with the Jail Commander/District Commander, or his designee, or the Sheriff's Office Facility Planning Coordinator prior to the commencement of the project.

NOTE: ENTRY AND EXIT COULD BE DELAYED DUE TO UNSCHEDULED INMATE MOVEMENT OR ACTIVITIES.

The time of entry and exit must be predetermined by the Jail Commander/District Commander or his designee who may consider a more flexible schedule. With the exception of delivery truck drivers, entry will not be granted to any person who is not in possession of a valid Sheriff's Office Facility Visitor Card or on the access list.

At the start of each workday (times will vary), all persons working on this project will enter the grounds at one time in the AM.

At the end of each workday (times will vary), all persons working on this project will exit the grounds at one time in the PM.

While it is suggested that all contractors bring their lunches, sodas, etc. with them when they enter the grounds each AM, they may depart the grounds for lunch if they so desire, however, they must ALL depart and return at the same time.

Port-A-Johns will need to be placed on the grounds by the contractor. An area will be decided by the Jail Commander/District Commander or his designee or the Sheriff's Office Facility Planning Coordinator.

Equipment, and Supplies, etc. may be brought in through the Facilities Vehicle gates. All Weapons and Alcohol are strictly prohibited on jail premises or grounds. Tobacco and tobacco products cannot be brought into the Facility.

The contractor must inventory all tools brought into the facility, before entering and departing the jail grounds. Copies must be provided to the Jail Staff. Contractors may leave tools on site provided they are locked up in a metal storage container in a location approved by the Jail Commander/District Commander or his designee.

Tools that are **NOT** being used must be kept in secured containers or within the immediate reach and control of the contractor.

Contractor personnel shall not operate any Sheriff's Office property.

CONTRACTOR MUST IMMEDIATELY REPORT ANY LOSSES OR UNEXPLAINED DAMAGE TO EQUIPMENT TO THE JAIL COMMANDER/OR THE DISTRICT COMMANDER.

Contractors will **NOT** talk to or associate with any inmate for any reason.

PART 3 - DISRUPTION TO ELECTRICAL SERVICE OR WATER SERVICE

We **MUST** have at least twenty-four (24) hours advance notice prior to the electricity or water being shut off **TO ANY AREA.**

The electricity or water service to only one (1) housing unit or building will be shut off at any time.

The length of time it is off is to be kept to the absolute minimum; however, it **MUST** never exceed four (4) hours in duration

PART 4 – KEYS

Keys will **NOT** be left in any vehicle or piece of equipment that is left unattended.

If a key is not required to start any vehicle or piece of equipment, that vehicle or equipment will be disabled so that an inmate will not be able to start it if it is not in the immediate control of a contractor.

PART 5 – VEHICLES

Only job essential vehicles may be brought onto the grounds. Note that these vehicles will remain on the grounds only long enough so that equipment, supplies, etc., may be loaded/unloaded.

Personal vehicles will not be allowed on the grounds.

Personal or contractor vehicles parked outside the grounds will not be parked within twenty (20) feet of any fence line or within fifty (50) feet of any fence line gate.

PART 6 – MECHANICAL PLANT

If cranes or other types of mechanical equipment are to be used or left unattended, a temporary fence must be erected up around them by the contractor.

Equipment and supplies will not be staged on grounds without prior approval from the Jail Commander/District Commander, or his designee.

PART 7 - EXCAVATION:

We **MUST** have a minimum of twenty-four (24) hours advance notice prior to any digging being done within any secured perimeter fencing.

Prior to any excavation, the specific location of underground utilities shall be marked. If there is any doubt of their location, the Facilities Management Project Manager shall be contacted. Any disruption to services will be repaired at the contractor's expense. All services must be back on-line prior to the contractor leaving for the day. There will be no exceptions.

The contractor shall be fully conversant of the location of **ALL** shut-off valves, (water and gas) and all electrical panels prior to commencing excavation.

All excavations **MUST** be properly marked during daylight hours and adequately illuminated and marked during the hours of darkness.

All excavations that go under any fence line or gate **MUST** be completely back filled and tamped or covered with a heavy steel plates that are secured to the ground except when the contractor is physically working in that excavated area.

AT NO TIME WILL A HOLE, TRENCH, ETC., THAT GOES UNDER A FENCE OR GATE BE LEFT UNCOVERED IF IT IS UNATTENDED BY THE CONTRACTOR.

Equipment and supplies shall **NOT** be left with twenty (20) feet of any fence or building.

Ladders used to access roofs shall **NOT** be left unattended. All ladders left on the job site shall be secured with a pad lock to prevent their use by unauthorized persons.

PART 8 – DISRUPTION TO FIRE ALARM SYSTEM

The fire alarm system can only be deactivated, reactivated or reset by Maricopa County's contracted fire alarm system vendor. The Contractor is to complete Section 00865, Fire System Bypass Request Form and submitted to the Facilities Management Project Manager three business days prior to the disabling of any fire alarm or sprinkler system. The contractor will be responsible for all vendor fees for services.

IF DIRECTED BY THE SHERIFF'S OFFICE STAFF, WORK MUST BE STOPPED: THIS ORDER MUST BE COMPLIED WITH AND CONTRACTORS MUST LEAVE IMMEDIATELY WITHOUT QUESTIONS, AS THE SAFETY OF THE CONTRACTORS AND THE STAFF COULD BE IN JEOPARDY.

BASED ON SECURITY AND SAFETY ISSUES, STRICTER CONTROLS MAY HAVE TO BE IMPLEMENTED; HOWEVER, THE JOB SUPERINTENDENT WILL BE ADVISED PRIOR TO ANY CHANGES BEING MADE.

EXHIBIT I**OET CABLING STANDARDS****A. Purpose**

The purpose of this document is to establish consistent, County-wide communications wiring installation standards for network cabling within Maricopa County facilities undergoing new construction and/or major renovations.

B. Reference

This document is based upon BICSI standards and references from the 2006 Telecommunications Distribution Methods Manual (Twelfth Edition, Volumes One & Two), along with applicable state and local codes and standards. MC-OET reserves the right to require more stringent standards where applicable.

C. Standard

All communications wiring plans for new construction and major renovations must comply with the requirements outlined in this document. In general, the Contractor shall be responsible for the installation, termination, testing and documentation of all specified communications cable.

All existing installations in the downtown campus use a Panduit solution with Category 6 cabling. Remote locations may use a Leviton solution with Category 6 cabling, unless a Panduit solution is already present. Verify product requirements specific to each site with the Maricopa County OET Program Manager, Infrastructure Project Manager, IT Senior Manager or MC-OET point of contact prior to placing any material orders.

Sumitomo tube cell and Air-blown fiber (ABF) is used to interconnect multiple closets within the same building and between floors. Manholes and vaults throughout the Maricopa County campuses will be connected with the appropriate type of tube cell and ABF.

At the completion of all projects, MC-OET reserves the right to require the Contractor to perform random tests witnessed by the Maricopa County Telecommunication Project Manager. Additional testing may be required if random testing determines that factory specifications have not been met. See Section 4: Testing, for specific test requirements and procedures.

At the completion of a work order or project, the Contractor shall provide the following documentation to MC-OET as specified in detail in Section 5, Deliverables:

- All as-built drawings will be done in CAD and shall be provided to MC-OET in an electronic format. Hard copies must be available upon request.
- As-built drawings must identify voice and data drops along with any cable pathways.
- Electronic copies of the test results for all copper and fiber installed.
- Copy of the warranty punch list developed by the contractor and the manufacturer during their initial walk-through.

The document is divided into six sections:

Section 1 – General Requirements

Section 2 - Horizontal Cabling

Section 3 - Vertical Cabling

Section 4 - Testing

Section 5 - Deliverables

Section 6 - Parts List

Section 1 describes standard cabling procedures which apply to any network cabling installation. Sections 2 and 3 are specific to the installation procedures and type of network being installed. Sections 4 and 5 relate to testing and final deliverables.

Section 6 lists the most common components used for the network installations.

SECTION 1: General Requirements

- A. A scope of work and work order number is required prior to authorization to proceed on any work. A Bill of Materials (BOM) must be submitted for all work orders larger than 10 drops. All other work orders performed shall contain a list of materials used. The list shall contain the vendor name (i.e. Panduit, Leviton, etc), a part number or description, and number or length of each item used (refer to Section 6, Parts List).

Contractors will maintain work site cleanliness at all times. All trash and garbage must be removed from the worksite daily. Beverage and food containers are not allowed in any of MC-OET Data Centers and or Equipment Rooms (ER)/Telecommunications Rooms (TR).

Materials purchased for the project or work order will only be unpackaged as needed.

Materials left after the completion of a project or work order must be returned to inventory. All items being returned must contain all parts – screws, labels, etc. (Parts must not be taken out of another box if a box has been opened and items are missing.)

Dirt and dust contamination can degrade fiber optic cable performance significantly. Fiber optic couplers and fiber optic patch cables shall be protected at all times prior to installation of the fiber optic patch cables by installing dust caps. Retain dust caps that are removed during the installation of the fiber patch cables, store in a suitable container, and place the container in the fiber termination enclosure.

Immediately replace dust caps on patch cables and couplers after any field changes to the network are completed.

Any fiber jumper not in-use shall be removed from the cable management, capped and returned to the inventory.

Removal of ceiling tile, drilling into cement walls, wood, or other materials within the room results in fine dust released into the air. Appropriate precautions are required to keep this dust from falling on or around any networking equipment installed in a telecommunications room. These precautions must be taken regardless of whether or not the equipment is activated. If the equipment is activated (operational), then additional care must be taken to ensure that air-flow is not restricted.

All changes made to the infrastructure shall be properly labeled and documented according to TIA/EIA 606-A Labeling Standard and County requirements. MC-OET requirements are provided in more detail under Section 5 – Deliverables.

All patch cords and fiber jumpers shall be 100% tested and certified by the manufacturer to meet or exceed the Category 6 copper and 10 Gigabit fiber standards. MC-OET may request supporting documentation published by the manufacturer. Channel testing shall not be permitted to ensure that copper patch cords and fiber jumpers independently meet the required performance standards of Category 6 copper or 10 Gigabit fiber.

As part of the project scope of work, MC-OET may require a percentage of horizontal cables to be channel tested after the installation process is complete.

The Leviton/Fluke JackRapid™ tool shall be used for all Leviton Quick Port CAT6 outlet module terminations. Use of any other tool to complete the termination process is prohibited.

Panduit Mini-Com® CAT6 outlet modules shall be terminated using the Panduit TGJT Termination Tool. Use of any other tool to complete the termination process is prohibited.

All work area locations will have three cable runs. Two (2) category 6 cables runs will be terminated for data. One (1) Category 3 cable run will be split and terminated to two (2) Category 3 USOC jacks for voice (refer to the horizontal cabling details in Section 2, Horizontal Cabling, before construction is started).

All coaxial cable will be installed as described in the project requirements of the scope of work (SOW).

See Section 4: Testing, for specific test requirements and procedures for testing.

The installation and test results will be verified by MC-OET Project Manager and/or Lead Technician.

CATV Applications- RG6, 18 AWG, quad shield, 75 ohm nominal impedance, copper clad steel center conductor with foam dielectric, 100% aluminum/polyester tape with a minimum of 60% aluminum braid shield. For CATV applications the maximum cable run length for RG6 cable should not exceed 150'.

When installing coaxial cable do not exceed the minimum bend radius requirements or the maximum pulling tension as specified by the cable manufacturer or permanent damage to the cable may occur. Cable damaged during the installation process shall be replaced at the contractor's expense.

F-type compression connectors shall be utilized for coaxial cable terminations.

At the completion of a project consisting of 30 or more drops, the contractor shall schedule a final walk-through with MC-OET Project Manager and/or Lead Technician. The cabling contractor will provide MC-OET with a timeline and plan for addressing any punch list or warranty items. In addition, a meeting shall be scheduled with the cabling vendor to conduct a walk-through to complete the warranty requirements.

TELECOMMUNICATIONS SPACES:

Telecommunications spaces are defined as:

- Telecommunications Room (TR)
- Equipment Room (ER)
- Entrance Facility (EF)

Considerations common to TRs, ERs, and EFs are shown in this section.

Telecommunications spaces shall be a rectangular room with minimum floor dimensions of 10 ft x 8 ft.

There shall be at least one ER or TR per floor. (TDMM, p. 6-23)

When the number of work areas to be served is known, the Telecommunications room floor space should be equal to 0.75 square feet of space multiplied by the number of work areas.

If the number of work areas is unknown, calculate the square footage of floor space required by dividing the amount of usable floor space by 100 ft² per 110 square feet of work area space served (TIA/EIA-569-A).

All Floors will have VCT Tile (Non-Static Preferred). Carpet as a floor covering is prohibited. Bare concrete is easily chipped creating dust particles which can cause damage to network equipment. Other treatments, paints or coatings for floors can be used if specifications indicate dust and static electricity are minimized with the particular type chosen. Floor coverings for telecommunications spaces must be approved by the Maricopa County OET Project Manager during the design phase of the project.

Install 4'x 8'x 3/4" fire retardant A/C grade or better, void-free plywood per TIA/EIA-569-A standards on 3 walls. The grade A side is the side exposed. (TDMM, page 6-19)

If approved by MC-OET, the plywood may be treated with at least two coats of fire retardant paint on all sides per TIA/EIA 569A standards instead of using fire retardant plywood.

Allow a minimum of 3.28 ft. wide x 3.28 ft. deep and 7.5 ft. high for equipment racks, cabinets and enclosures. Allow a minimum of 3.28 ft. of aisle space in-front of and to the rear of the space allocated for the equipment racks, cabinets or enclosures. (TDMM, p. 6-47)

One or more load bearing walls should be incorporated into the design of all Telecommunications Spaces. This reduces the possibility of relocating the telecommunications space if the floor or building is expanded or altered in the future. (TDMM, p. 6-13)

Sleeves, slots and conduits should be located on the left side of the room to enhance left to right expansion.

Telecommunications spaces shall be dedicated for telecommunications use. Do not locate building custodial services (sinks, cleaning materials, mops, electrical system transformers, sources of EMI, etc.) in Telecommunications spaces.

ENVIRONMENTAL CONTROL FOR ER'S AND TR'S

Maintain room temperature between 64 degrees and 75 degrees (F) with relative humidity range from 30 % to 55% (non-condensing). This should be maintained constantly 24 hours by 7 days a week. BTU requirements will be established based on equipment to be installed. If no active equipment is located in the room, temperature may vary from 50 - 95°F. (TDMM, pages 6-10 and 6-55)

ELECTRICAL POWER FOR ER'S AND TR'S

New Construction Projects or existing County buildings involved in the infrastructure upgrade will require electrical power to support the equipment being installed, and to ensure redundancy.

The following sections list the minimum power requirements for ERs and TRs. Additional electrical power requirements may be applicable depending on but not limited to factors such as on the size and shape of the ER/TR and additional equipment requirements.

Verify all power requirements including but not limited to the location of the outlets and quantity of circuits required with the OET project manager prior to installation.

Convenience Outlets.

At least two (2) duplex non-switched 120VAC electrical outlets (NEMA 5-20R) located on opposite walls for tools and test equipment and placed on a separate circuit from those serving the Telecommunications equipment are required for each ER/TR. (TDMM, page 7-10).

Catalyst 6500 series and 4500 series equipment power requirements

Each Catalyst 6500 series and Catalyst 4500 series chassis is installed with two (2) power supplies.

Two (2) 20A, 250VAC, separate and dedicated branch circuits with NEMA 6-20R grounded receptacles and protected by separate two-pole circuit breakers are required for each chassis. Allow for a minimum of two (2) 6500/4500 series chassis to be placed in each TR/ER.

The source AC outlets must be within 6' of the system and easily accessible. Outlets shall be located on the outside of the cable support tray unless otherwise noted.

AC-input power supplies require single-phase source AC.

All AC power supply inputs shall be fully isolated.

UPS models utilizing ferroresonant technology shall not be utilized with the 6500 series chassis. Some uninterruptible power supply (UPS) models that use ferroresonant technology can become unstable when operating with the Catalyst 6500 series switch power supplies which use power factor correction (PFC). This can cause the output voltage waveform to the switch to become distorted resulting in an undervoltage situation in the system.

Catalyst 3750 series equipment power requirements

Each Catalyst 3750 is installed with two (2) power supplies.

Two (2) 20A, 125VAC separate and dedicated branch circuits with NEMA 5-20R power receptacles are required for each power supply. Allow for a minimum of one (1) 3750 series chassis to be placed in each TR/ER.

The source AC outlets must be within 6' of the system and easily accessible. Outlets shall be located on the outside of the cable support tray unless otherwise noted.

AC-input power supplies require single-phase source AC.

All AC power supply inputs shall be fully isolated.

CONDUIT REQUIREMENTS FOR ER'S AND TR'S

Maricopa County requires a minimum of two 4" conduits from the Entrance Facility (EF) to the property line for QWEST, and two 2" conduits for COX. Additional conduits may be specified to support Enterprise Network Core and Data Center Locations.

The size and number of conduits or sleeves used for backbone pathways depends on the usable floor space served by the backbone system. However, at least four 4 inch conduits are recommended to serve a Telecommunications Room (TR), Equipment Room (ER), or Entrance Facility (EF). (TDMM, page 6-8)

Multiple Telecommunications rooms on the same floor shall be interconnected with a minimum of two 4" conduits.

For horizontal station cabling, twelve inch cable tray should be substituted for conduit whenever possible. A minimum of one 4 inch EMT sleeve will be installed in all Telecommunication Rooms in order to route-in horizontal station cables.

All sleeves and slots must be firestopped in accordance with applicable building codes after the cable installation is complete.

If possible, sleeves, slots, and/or conduits should be located on the left side of the Telecommunications Spaces. This placement enhances the use of wall space from left to right.

All conduit installed shall have the appropriate size bushings placed on the top and bottom of the sleeve to protect the cables.

Interconnecting buildings in a campus environment requires a minimum of three 4" conduits.

EQUIPMENT ROOM – ER (Formerly MDF):

The size of the Equipment Room (ER) shall be determined as a joint effort between the Maricopa County OET Project Manager, building owner and other parties designated by MC-OET. The Equipment Room size cannot be specified until all factors relating to the work space area and equipment are considered. (TDMM, p. 6-45)

If less than 200 Work Area's, minimum ER size = 160 ft^2 (15m^2).

A space with the minimum floor dimensions of 10 ft. x 16 ft. (160 ft^2) should be allocated for the Equipment Room (ER) (TDMM, p. 6-43)

For buildings less than 5000 square feet a room 10 ft x 8 ft may be utilized. (TDMM, p. 6-15)

Provide an unobstructed clearance of a least 8' 6" above the finished floor. The door must be at least 7' high and 3' wide. Doors shall have the same fire rating as the walls in the room. (TDMM, p. 6-8)

Since large equipment is often located in the ER, a double door (e.g. 6 feet wide by 7.5 feet high) may be required. If building codes permit, doors should open outward to provide additional usable space and reduce constraints on telecommunications spaces layout. Contact the Maricopa County OET Project Manager for project specific door requirements during the design phase of the project. (TDMM, p. 6-8)

The rating for concentrated loading must be greater than 2000 pounds per square foot in areas that will support telecommunications equipment. The actual floor-load rating should be obtained from the building architect before construction is started. (TDMM, page 6-56)

TELECOMMUNICATIONS ROOM – TR (formerly IDF):

Floor Size	Minimum Room Size
< 5,000 ft^2	10 ft x 8 ft
>5,000 to 8,000 ft^2	10 ft x 9 ft
>8,000 to 10,000 ft^2	10 ft x 11 ft

BONDING AND GROUNDING REQUIREMENTS

General Requirements:

A uniform telecommunications grounding and bonding infrastructure shall be provided for the protection of personnel and equipment conforming to all applicable codes and standards including, but not limited to the following: the current National Electric Code (NEC) Articles 250 (Grounding) and 800 (Communications Circuits), ANSI/J-STD-607-B-2011, Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications., IEEE 1100 "Recommended Practice for Powering and Grounding Electronic Equipment", TIA/EIA-942 "Telecommunications Infrastructure Standard for Data Centers", and the current versions of the National Fire Protection Association (NFPA) publications NFPA 70E "Electrical Safety Requirements for Employee Workplaces", NFPA 75 "Protection of Electronic Computer/Data Processing Equipment", ANSI/NECA/BICSI-607, Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings, 2010 and NFPA 780 "Lightning Protection Code". These are minimum requirements and do not replace federal, state, local, or other applicable codes, laws, or regulations which may have priority. Conflicts between this document, local safety code, BICSI guidelines, and manufacturer's requirements should be resolved with the AHJ before proceeding.

Splices in bonding or grounding conductors are not allowed.

All bus bars will be located 18 inches above the floor.

The elements defined by the ANSI/TIA/EIA-607-A and IEEE1100 standards are listed below:

TMGB	Telecommunications Main Grounding Bus Bar
TGB	Telecommunications Grounding Bus Bar
TBB	Telecommunications Bonding Backbone
TBBIBC	Telecommunications Bonding Backbone Interconnecting Bonding Conductor
BCT	Bonding Conductor for Telecommunications

Telecommunications bonding to electrical ground:

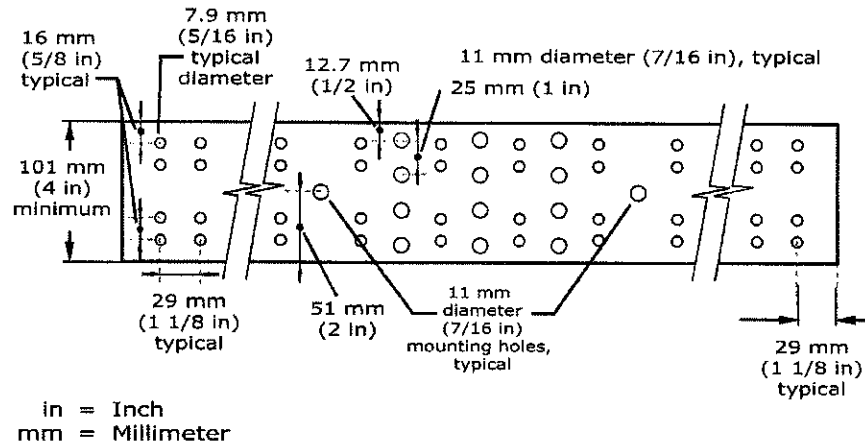
The Telecommunications Main Grounding Bus Bar (TMGB) will be interconnected with the building's service equipment (power) ground using a Bonding Conductor for Telecommunications (BCT) as large as a No. 3/0 AWG. The conductor must be at least one size larger than the Telecommunications Bonding Backbone (TBB).

IMPORTANT: The TBB is a bonding conductor intended to equalize potentials between TRs on multiple floors of a building with an ultimate connection to the Entrance Facility's (EF) TMGB. TBB installations for large sites may be too costly to achieve. As an alternative, the TGB in each TR may be bonded to the AC electrical panel for that floor of the building with a supplemental bonding connection made to the metal frame of the building, where applicable. Each of the bonding connections must be tested to verify that a low resistance connection exists. (TDMM, p. 9-19)

The Telecommunications Main Grounding Bus Bar (TMGB) serves as the dedicated extension of the building grounding electrode system for telecommunications infrastructure. The TMGB also serves as the central attachment point for the Telecommunications Bonding Backbone (TBB) and equipment, and MUST be accessible to telecommunications personnel. The TMGB must be mounted as close as possible to the cable Entrance Facility (EF). (TDMM, p.9-16)

The TMGB shall be:

- A predrilled copper bus bar provided with standard NEMA bolt hole sizing and spacing for the type of conductor to be used.
- Sized in accordance with the immediate requirements of the application and allow for the consideration of future growth.
- Have a minimum dimension of ¼ in thick x 4 in wide and variable in length.
- Insulated from its support; a 2" separation is recommended.
- Listed by an NTRL.



If the main AC service entrance panel is less than 30 feet from the TMGB, bond the TMGB to the AC grounding electrode of the panel using a bonding conductor for telecommunications (BTC). (TDMM, p.9-16)

A Telecommunications Grounding Bus Bar (TGB) must be placed in each telecommunications room and equipment room and bonded by means of the telecommunications bonding backbone conductor to the Telecommunications Main Grounding Bus Bar (TMGB). The TGB should be referenced to the equipment ground terminal of the nearest AC electrical panel board to equalize potentials between them. This panel board (known as a branch circuit panel board) may reside in the ER. Also, the TGB should be bonded to the nearest structural steel member (if available) whether it is a horizontal or vertical beam. (TDMM, pp. 8-18 and 8-19)

The TGB shall:

- be a predrilled copper bus bar provided with standard NEMA bolt hole sizing and spacing for the type of conductor to be used.
- be sized in accordance with the immediate requirements of the application and allow for the consideration of future growth.
- have a minimum dimension of ¼ in thick x 2 in wide and variable in length.
- be insulated from its support; a 2" separation is recommended.

The Telecommunications Bonding Backbone (TBB) cables for bonding the TGBs to the TMGB shall be sized according to length, as shown in the chart below:

Sizing of the TBB	
TBB Length Linear M (ft)	TBB Size (AWG)
Less than 4 (13)	6
4 – 6 (14 – 20)	4
6 – 8 (21 – 26)	3
8 – 10 (27 – 33)	2
10 – 13 (34 – 41)	1
13 – 16 (43 – 52)	1/0
16 – 20 (53-66)	2/0
Greater than 20 (66)	3/0

All Telecommunication Rooms (TR) shall have a minimum 6 AWG bonding conductor extending from the TGB to all the racks and cabinets within the TR. This 6 AWG conductor will be referred to as the common bonding network (as referred to in TIA-942 "Telecommunications Infrastructure Standard for Data Centers").

All racks and cabinet frames will be fully bonded with paint piercing washers and bonding screws and attached to the common bonding network with a minimum 6 AWG conductor. In order to fully bond all equipment and panels to the rack, thread-forming screws must be utilized to ensure clean metal to metal contacts. **SELF-TAPPING SCREWS SHOULD NEVER BE USED BECAUSE THEY CREATE METAL SHAVINGS WHICH CAN DAMAGE THE ELECTONICS.** Two-hole grounding lugs will be used for the rack grounding bus bars. One-hole grounding lugs are prohibited.

Each rack or cabinet shall have at least one ESD port and ESD strap provided on the front of the rack.

In cases where both ends of a cable cannot be visually located at the same time, green labels shall be utilized for visual inspection of the grounding and bonding system. This labeling will be reflected on the as-built drawings referenced in the Deliverables, Section 5 of this document.

DATA CENTER GROUNDING REQUIREMENTS:

Proper grounding within a data center is defined by TIA/EIA-942 "Telecommunications Infrastructure Standard for Data Centers", J-STD-607-A, IEEE Std 1100 (IEEE Emerald Book) and BICSI TDMM Manual. The TIA/EIA-942 standard goes beyond the requirements of the National Electrical Code (NEC) to protect equipment and improve system reliability.

The goals of the grounding system in a data center are to equalize electrical potentials and to create a low resistance path to ground. Five basic principles should be used when designing a grounding system to accomplish this goal, as follows:

1. The grounding system shall be intentional.
2. The grounding system shall be visually verifiable.
3. The grounding system shall be adequately sized.
4. The grounding system shall direct damaging currents away from equipment.
5. All metallic components in the data center shall be bonded to the grounding system.

All bonding and grounding design and requirements shall be reviewed and approved by the Maricopa County OET Project Manager before implementation.

SIGNAL REFERENCE GRID (SRG)

The Signal Reference Grid has three purposes:

1. Reduce electrical noises and enhance the reliability of signal transfer across interconnected items of IT equipment.
2. Prevent circuit damage by providing a low impedance path/effective ground reference for computer room electrical equipment.
3. Minimize damage to circuits and equipment when a power system ground-fault event occurs.

Best practices for the Signal Reference Grid include:

1. The SRG should be prefabricated out of #26 gauge x 2 in. wide copper strip with all crossing interconnections welded, not punched.
2. If round conductors are used, they should be at least # 6 AWG; bare copper is preferred.
3. The grid spacing of the SRG should be 2 feet, exothermically welded in the field to form a continuous grid.
4. The copper strips can be welded into a grid pattern prior to installation and then rolled out onto the floor in sections.
5. When a wire SRG is constructed using the raised floor pedestals, the flooring system must be electrically continuous.
6. Every fourth pedestal should be bonded.
7. The bonding jumper from the pedestal to the SRG should be no greater than 2 feet in length.

Best practices for Rack/Cabinet grounding include:

1. All none-current-carrying metallic enclosures shall be grounded.
2. Each equipment cabinet/rack requires its own grounding connection to the SRG.
3. A minimum of #6 AWG copper conductor mechanically terminated to the SRG and cabinet via a machine screw, through-bolt connection or factory-provided spot weld, is recommended.
4. Grounds at opposite ends of a series of racks should be attached with the framework grounding conductor going directly to the SRG.
5. Bare metal-to-metal contact is mandatory for all bonded connections, with anti-oxidant applied at the connection point. (BICSI Data Center Design and Best Practices, version 1.1, pp. 8-53, 8-55)

SECTION 2: Horizontal Cabling

All horizontal distribution cabling shall be plenum rated.

Horizontal Cabling-Data/VoIP

Data and VoIP applications shall utilize 4-pair, 100 ohm, CAT6 UTP, CMP cable.

Horizontal Cabling-Voice

Horizontal distribution supporting digital and analog voice applications shall utilize 4-pair, 100 ohm, Category 3, UTP, CMP cable. 4-pair, 100 ohm Category 5e UTP, CMP cable is an acceptable substitution. Typical services would include but not be limited to connections to legacy telephone systems, fax, elevator phone, and telephone lines for monitoring alarm systems.

Cable Routing

Horizontal cabling shall be installed from the workstation to the nearest floor serving TR or ER. No station cabling will run between floors. Exceptions may be required based on specific site conditions and project requirements. All exceptions must be approved in advance prior to installation and authorized in writing by the OET Project Manager.

Route cabling so that a minimum distance of 12" is maintained between any network cabling and florescent lighting fixtures. Under no circumstances shall network cables be installed physically touching florescent lighting fixtures.

Avoid routes that take cabling near sources of high electromagnetic radiation, electrostatic discharge, or radiated frequency (RF) interference. Devices such as electric motors or RF generating equipment may generate electrical emissions. When in doubt, check with the manufacturer of the equipment. The network may appear to function normally but problems will occur as size and network traffic increase.

Cables installed in removable tile suspended ceiling areas shall not rest on the ceiling grids. Cables should be routed to provide the maximum clearance above the ceiling tiles. The Minimum clearance is at least 3 inches above the ceiling tiles.

Horizontally installed cables in removable tile suspended ceiling areas will be supported by cable tray for main cable runs and J-hooks for independent cable drop locations. Where cable tray is utilized, 12 inches of clearance should be provided above the cable tray. All metal trays should be bonded back to the common bonding network as described under the Grounding and Bonding subsection of this document.

Velcro shall be used at spacing of intervals of 5 feet or less. Cable bundles shall be attached with Velcro only to hangers permanently affixed to the underside of the floor above. Cable bundles may be attached to existing ceiling grid support wires provided the cable bundles do not exceed a combined per foot weight of 0.5 lb per foot.

Cable may be installed using roof trusses as supports. The use of either hammer-on or screw-on beam style J-hooks is recommended. In situations where the installation of grid wire for J-hook support is being considered, consult with County Management for permission and time frame to complete this work.

Existing pipes carrying liquids or gases, electrical conduits or existing cabling, shall not be used to support horizontal cables. Cable routes should not be close to any pipes or ducts which vary from ambient temperatures. Cables should be routed as high as possible above pipes and not below.

Horizontal cables running parallel to electrical conduits shall not be tie-wrapped to the conduits. The network cable bundles shall be separated by a minimum of 3" of free air space from the electrical conduits.

Cable pulls shall not exceed the manufacturer specifications for the pulling tension or the bend radius. The maximum pulling tension of 25 lbs as referenced by the TIA/EIA-568-B shall not be exceeded. Cable pulls shall not be stretched, crimped or compressed during installation. Pull-strings should be provided in every pathway with more than 20 cables.

All horizontal or vertically installed cable that is penetrating fire walls or floor levels shall be sealed using an approved firestop compound and installed in compliance with local building codes. All fire walls will be penetrated with an elastomeric module of which one to eight can be installed with one housing frame. The elastomeric modules are specially designed to withstand the fire and hose stream test for the rated time. Frame and hardware components must be steel to survive test temperatures. An example is the Specified Technologies Incorporated EZ-Path® System Solution.

All network cabling shall be installed in straight-runs parallel to building lines. When changing the direction of a cable run, a smooth 90 degree turn shall be used that adheres to the cable manufacturers minimum bend radius without kinking or damaging the cable outer jacket or conductors.

The cable bend radius will not exceed 8 times the cable diameter or approximately a 2" bend radius.

A service loop will be provided at each end of the cable run. The length of the service loop shall be 5 feet at the station end and 10 feet at the ER/TR end. The service loop will not overlap in a figure 8 or coil pattern within the cable or ladder tray. The cable shall be transitioned and dressed-in the cable or ladder tray. This additional length shall extend in a U-shaped, non-overlapping loop with the proper bend radius maintained.

For situations where cable or ladder tray are not available or not of adequate length (e.g., J-hook installations), consult with the Maricopa County OET Project Manager. The use of a coil pattern for a service loop is prohibited.

Category 6

The maximum length from the network device to the network interface at the workstation end shall not exceed 328 cable feet when using Category 6 cabling. This maximum length includes the horizontal cable run and the patch cables installed from the switch to the patch panel and the workstation to the data jack in the faceplate.

The switch to switch maximum distance shall not exceed 328 cable feet when using Category 6 cabling including any patch or line cords.

The Category 6 cable shall not exceed the specifications for the specific topology being installed.

The cable run shall have no splices.

The cables will not be "cinched" with tie-wrap cable ties or any other device used to support the cables in the overhead ceiling space. Velcro ONLY shall be used.

Due to the "crushing" effect from the weight, cable will not be run in bundles greater than 120 cables. In addition, cables should be bundled so that no more than 10 work areas are located in the same cable bundle to facilitate MAC work in the future.

All terminations will follow Category 6 specifications and be Category 6 compliant. Proper termination tools will be used for the specific vendor product being installed. Patch panels and all station locations will use Panduit's Category 6 RJ45 red or Leviton's dark red jacks for all data drops.

All cable pulls shall be labeled according to the labeling standards. All cables will be labeled approximately 6" inches from the jack.

Category 3

Category 3 cabling shall be used for voice locations ONLY. Category 5e cable can be substituted if cost is less than or equal to Category 3 cable. Sites that migrate to a VOIP solution will use Category 6 cabling and those standards will apply.

No more than 1 1/2 inches of outer jacket shall be removed at ANY termination point.

The cable bend radius will not exceed 8 times the cable diameter.

The cable run shall have no splices, "T"s, or bridge taps.

Station Termination

All station locations will have a single gang 4-port faceplate with two Category 6 cables and one Category 3 cable. The Category 6 cables will be terminated with Cat6 Red Panduit RJ45 or Dark Red Leviton jacks. The Category 3 cable will be terminated with two Category 3 Panduit Electric Ivory or Leviton Ivory USOC jacks. The faceplates are Electrical Ivory for Panduit and Ivory for Leviton. The TIA/EIA 568-B cabling standard will be used for cable termination.

All empty ports in a faceplate will have the appropriately colored blank insert installed.

Each drop location will be installed in a 1 inch EMT conduit leading back to the nearest cable tray. Each conduit will be labeled and located approximately 6 inches above the cable tray. The conduit shall contain a pull-string which ends in a 2.25 inch deep x 4 inch square box. The conduit shall enter the 2.25 inch deep x 4 inch square box from the top if the cable is coming from the ceiling and from the side if the cable is coming from a horizontal location. No 90 degree elbows shall be used to connect the conduit to the box. A metallic cover for the box will be installed to reduce the box size to accommodate a single gang faceplate.

All faceplates will be mounted level. The bottom of the faceplate will be EXACTLY 11 ½" from the floor. If the new faceplate is placed next to an existing outlet it should be placed level and square with the existing faceplate.

All faceplates will be snug and tight with the wall and when mounted correctly, the faceplate will not move.

A minimum of 12 inches and a maximum of 24 inches of slack should be located in the cable tray but accessible for any re-terminations required.

All cables will be labeled approximately 6" inches from the jack including the patch panel end.

All faceplates will be labeled as detailed in the "labeling section" in this document.

ER/TR Termination

A minimum of one 19" rack with vertical cable management is required in each TR or ER. The 19" rack will support all station cables terminated to Category 6 patch panels. All station cable will enter the TR/ER through 4" conduit sleeves or cable tray and will be transitioned to ladder tray to the appropriate termination location. The cable should be properly bundled with Velcro. Vertical cable managers shall be installed on both sides of the rack. Cabling shall be equally distributed to both sides of the rack. As an example: when facing the rack, cable runs 1 – 12 and 25 – 36 should be to the left side of the rack. Cable runs 13 – 24 and 37 – 48 should be to the right side of the rack.

Four-inch, single-sided horizontal managers shall be installed as "pass-throughs" in the middle of the rack to provide a path for patch cables to be routed to the opposite side of the rack. Forty-eight port angled patch panels shall be used in most installations. Unused ports on the patch panels shall be plugged with a blank insert matching the color of the patch panel. Two-inch, single-sided horizontal managers may be used if approved by the Maricopa County OET Project Manager.

The use of angled patch panels does not require horizontal cable managers.

Waterfalls shall be installed for cable entry from the ladder tray to the vertical cable management. All station cables will maintain the same esthetics and bend radius and not overlap one another. All patch panels will have strain relief bars mounted on the rear of the rack for cable support.

All Category 3 cable will be terminated on a 110-type termination block.

All cable entering termination blocks must enter from the top. Cable managers will be installed with the 110-type termination block.

All network cabling shall be supported by ladder tray. Copper riser cabling shall be supported by D-Rings. Where fiber and copper jumpers share the same ladder tray, the fiber shall be kept to one side and copper to the opposite side. The cable shall be properly bundled with Velcro.

All 110-style punchdown blocks, cable managers and patch panels shall be mounted square and level.

The 110-type punchdown block will be used for all feeder/backbone copper and category 3 station cables. All cable shall be labeled with clear designation strips and computer or label maker printed labels. Color-codes for labeling must be adhered to.

All patch panels will be labeled with label maker type labels.

Backboard Layout – The following diagram provides the layout of the backboard cross-connect fields.

CABLE MANAGEMENT						
300/900 Pair 110 Tower	Cable Management	300/900 Pair 110 Tower	Cable Management	300/900 Pair 110 Tower	Cable Management	300/900 Pair 110 Tower
Qwest Feed		Floor Riser		Station Cable		IPE Voice Cables

The following colored labels will be used to identify cable termination types within the telecommunications room and is the code recommended in the TIA/EIA 606-A standard:

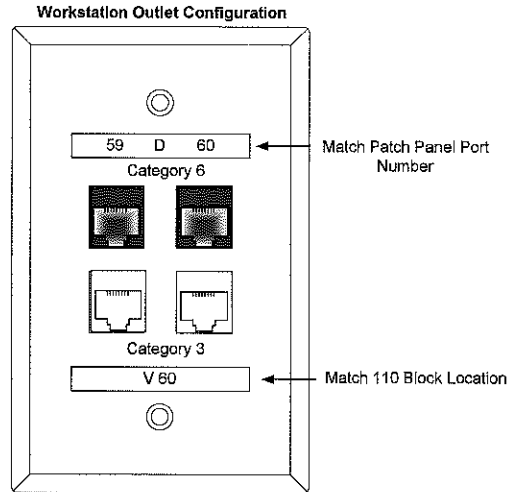
Blue	Horizontal station cables
White	Riser cable
Gray	second level backbone or riser cable
Brown	Inter-building backbone cable
Purple	Common Equipment ports (IPE)
Green	Customer extension of demarcation
Orange	Service provider demarcation
Yellow	Auxiliary circuits, alarms, security
Red	Key telephone systems

LABELING

Station cables shall be labeled at all termination points including the TR/ER and workstation outlet locations. A black on Yellow wrap around label will be put on each end of the cables and approximately 4-6 inches from the patch panel. Each jack at each workstation outlet shall have an individual identification number. This number shall be carried through to the TR/ER and any other points of termination that may exist.

The upper and lower designation strip will be applied to the faceplate. A label machine using a 3/8" cassette tape, black on white background will be used to print the labels. Patch Panels shall be labeled using a labeling machine which prints the appropriate sized labels for the patch panel used or a label machine using a 3/8" cassette tape, black on white background. Port numbers should line up with the jack to which it is assigned.

The following is an example of a wall plate with labels corresponding to patch panel labeled ports.



Floors with more than one TR will require that the TR letter designation is added to the jack ID number (example A59 or B59). The statement of work shall reflect the closet numbering scheme used. If there is no reference in the scope of work, the Maricopa County OET Project Manager or Lead Technician shall be consulted.

For ABF installations, each tube exiting the TDU shall be labeled on the tube clip organizer indicating the tube number, the LIU, and the fiber adapter panel locations. Each tube entering the LIU shall be labeled with its source information back to the TDU. Exact labeling requirements will be specified by the Maricopa County OET Project Manager.

SECTION 3: Vertical Cabling

All Telecommunication Rooms will have a minimum of a 50 pair copper backbone cable run from the ER. It will be terminated on a 110 style punchdown block for existing phone service.

Proper grounding as described in the Bonding and Grounding Requirements in Section 1 will be adhered to for all copper backbone cabling. Circuit Protector Blocks with gas modules will be used in the ER where the transition from OSP to Plenum occurs within 50 feet of the entrance. The requirements of the NEC and local building codes must be adhered to. (TDMM, p. 5-69 states: "Chapters 7 and 8 of the NEC impose specific requirements for building backbone systems used within the United States...requirements are designed to prevent the spread of flame and smoke from floor to floor, and relate to backbone systems applicable to the ER, TR, EF, and TE...")

All TR's will have a minimum of 24 strands of multimode fiber for network equipment connectivity. This fiber will be 50 micron Laser Optimized Fiber specified with OFS glass capable of supporting 10 gigabit to 300m (OM3) or 550m (OM4) based on the length of the fiber. All fiber installations will be Sumitomo tube cell and Air-blown fiber (ABF). For smaller installations, non-ABF fiber may be used. The Maricopa County OET Project Manager will determine which type of fiber will be installed.

A service loop will be provided at each end of a fiber run. The length of the service loop will be 10 feet at each end. The proper bend radius shall be maintained.

All single mode and multimode fiber will be terminated on to a rack mounted LIU unless the project warrants otherwise. The Maricopa County OET Project Manager will make that determination. All vendor product determinations should be verified by the Maricopa County OET Program Manager or Lead Technician.

All fiber terminations shall be done with LC connectors, unless otherwise noted by the Maricopa County OET Project Manager or Lead Technician.

All non-ABF fiber optic cable will be installed in a protective innerduct. A plenum rating must be met if the innerduct is to be installed in a plenum environment. Check local building codes for verification. Armor protected fiber may be used in lieu of innerduct.

All ABF product installations shall be done according to manufacturer and County standards by certified installers. All test results shall be done according to the warranty requirements specified by the manufacturer.

All vertical cables penetrating fire walls or floor levels shall be sealed using an approved firestop compound and comply with all local building codes.

Sumitomo Air Blown Fiber:

All Air-Blown fiber shall be Sumitomo product and installed to Sumitomo standards by certified installers. Test results will be provided to the Maricopa County OET Project Manager upon completion of the installation. This shall be provided in a readable electronic format.

The Sumitomo Future Flex Enclosure will be used by Maricopa County. An alternative for this enclosure is the Hoffman enclosure. The Maricopa County OET Project Manager will determine the size and type of enclosure used on a per installation basis.

Sumitomo OSP Tube cell shall be installed in underground conduits. A Sumitomo or Hoffman waterproof enclosure 24"x12"x24" will be used in manholes and vaults (size may vary depending on location). All tube cells will be properly identified with a Plastic 2"x4" engraved label.

All AFB tube cable and fiber bundle shall be installed according to the recommended installation procedures provided by Sumitomo. Some of these installation procedures are listed below. This list is not considered comprehensive and therefore does not exclude all the applicable manufacturer's installation procedures.

All tube cells shall be installed in a manner which provides the straightest route and fewest bends possible. Tight bends and sharp S-curves must be avoided.

Proper reel handling and storage shall be followed for all Sumitomo tube cell cable.

A visual receipt inspection of the reel and contents shall be performed. If damaged is noted, the appropriate authority shall be notified immediately. An on-reel obstruction test is strongly recommended for all tubes. Document the test results and re-seal the tube cable ends.

Maximum allowable pulling tension shall be followed during any tube cable installation. Refer to the Sumitomo documentation guide for the specific pulling tension for the type of tube cell being installed.

To prevent deformation of the tubes by sagging or pinch points along the route, the tube cell installation shall be done according to the installation standards provided by Sumitomo. The following installation standards are provided for a brief overview. The contractor is responsible for ensuring all installation procedures are followed to ensure the tube cell cable is not damaged during or after installation.

For cable tray installations – solid tray or tray with flat inserts in the bottom is the preferred method for TP2 tube. Ladder tray may be used if the spacing between the ladder rungs is no more than 12" apart and the rungs are at least 1" wide. Flex-wire basket tray may be used as long as the basket mesh size is no more than 4" long and 2" wide. For any trays that do not meet the above requirements, a flat insert must be inserted across the rungs or in the bottom of the tray to provide a flat and continuous support for the tube cell.

Adjustable cable supports that utilize a cloth or fabric type strap ARE NOT acceptable support methods for TP2 tube cables.

J-hooks by themselves are NOT acceptable methods of support. J-hooks must be spaced no more than 4-to-5 feet apart and a minimum 10 to 12 inch long piece of innerduct is placed around the tube cable as it lays in each J-hook. The innerduct must be centered in the hook to provide the best support. The tube cable shall have no more than 6" sag between the J-hooks. Plenum-rated, corrugated split innerduct shall be used. Required sizes are – Carlon Electrical Division 1-1/4" Orange, Split CF4X1-250S (or equal) for 1" OD TCO7TP2 and Carlon Electrical Division 2" Plenum-rated Orange, split CF4X10250S (or equal) for 1.7" OD TC19TP2. Ensure the "split" points upward during the installation.

Velcro strapping shall be the only material used to secure TP2 Tube cable in place. However, Velcro strapping should NOT be used to support the weight of the tube cable at the narrow point load on the tubes. This will cause deformation. Nylon Tie-wraps are NEVER to be used.

Appropriate support for the tube cable shall be provided when TP2 tube cable transitions on and off a cable, ladder or flex-wire tray. This support shall adhere to the installation standards provided by Sumitomo.

The placement and stacking of tube cable shall be done according to the installation procedures provided by Sumitomo.

Manual installation of TP2 tube cable is preferred, if pulling ropes or strings are used, a swivel should ALWAYS be used between the cable grip and the pulling rope to prevent the cable from twisting.

Once the TP2 tube cable has been installed, the route should be re-inspected to correct any potential problems; add the split innerduct support if J-hooks were used; verify the sag is 6" or less and that the tube cable is not in contact with any sharp edges or points.

If TC07TP2 is used, verify the cable is laying on the flat surface and not the points.

All tube cells will be supported with Kellems Grips for bottom tube entries and plastic bushings on top of enclosure. Hose Clamps are not acceptable to MC-OET to support Tube cells in the enclosure even if Sumitomo would warranty it. All tube cells will be supported with appropriate 1-hole C-Clamps or D-rings to provide support as the tube exits the conduit and enters the TDU. Care should be taken to obtain the proper size clamp or D-ring so the tube cells do not get damaged.

All Sumitomo fiber bundles that are to be uninstalled shall be removed following the proper procedures outlined by Sumitomo. The fiber bundle shall be re-rolled on an appropriate size reel as specified by the Sumitomo standards.

All Sumitomo tube cell cables in stock shall be stored according to the Sumitomo standards.

SECTION 4: Testing

All technicians shall be trained and certified by the manufacturer or a designated representative of the manufacturer on the testing equipment used.

An electronic version of the test results in PDF file format shall be submitted to the "Office of Enterprise Technology" as part of the deliverables listed in Section 5. Test results from major projects shall be submitted on "readable" CDs.

Final test submittals shall not include failing test results. Cables that fail testing shall be repaired or replaced and re-tested until 100 percent of the cabling passes all testing.

A. Horizontal Copper Cabling

1. CATEGORY 5E AND 6 horizontal cabling shall be tested as recommended in the ANSI/EIA/TIA 586-C.2 Telecommunications Standard.
2. The installed twisted-pair horizontal links shall be tested from the IDF in the telecommunications room to the telecommunication wall outlet in the work area for compliance with the "Permanent Link" performance specification as defined in the TIA CATEGORY 5E AND 6 Standard using a Fluke DTX CableAnalyzer Series cable tester or County approved test equipment in compliance with ANSI/TIA-1152.
3. Submit detailed test results in electronic media in PDF file format.

B. Optical Fiber Cabling

1. Initially test optical cable with a light source and power meter utilizing procedures as stated in ANSI/TIA/EIA-526-14A: OFSTP-14A Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant and ANSI/TIA/EIA-526-7 Measurement of Optical Power Loss of Installed Single mode Fiber Cable Plant. Measured results shall be plus/minus 1 dB of submitted loss budget calculations. If loss figures are outside this range, test cable with optical time domain reflectometer to determine cause of variation.
2. Cables shall be tested at 850 and 1300 nm for multimode optical fiber cables. Cables shall be tested at 1310 and 1550 nm for single mode optical fibers.
3. Testing procedures shall utilize "Method B" – One jumper reference.
4. Bi-directional testing of optical fibers is required.
5. Submit detailed test results in electronic media in PDF file format.

Voice cables shall be tested with a mod-tap tester.

Software related to the specific cable tester used must be provided to MC-OET by the Contractor so that the test results can be read (readable format).

Copper Riser cable tests shall be from the TR termination blocks or patch panels to the ER termination blocks or patch panels. A continuity test is required upon completion of the installation.

Final System Test results of riser cabling shall be documented and provided to the "Office of Enterprise Technology" at final acceptance of the completed project, along with as-built drawings and other required documentation. This shall be provided in a readable electronic format.

All fiber optic cable strands shall be tested using a calibrated fiber tester approved by the Maricopa County OET Project Manager prior to installation to ensure all strands are continuous and match published specifications. If calibration is required for the tester, verification must be provided upon request.

All terminated fiber optic cable strands shall be tested using calibrated fiber testers approved by the Maricopa County OET Project Manager. The maximum db loss per strand is as follows:

ST Connector .2db
SC Connectors .2db
LC Connectors .2db

For non-ABF fiber, defective strands revealed in the testing procedure will be repaired and or replaced prior to final acceptance of the completed project. Repair of existing fiber that has been damaged, may be done with a Fusion Splice. No Mechanical splices will be accepted. All splices will be installed in the appropriate enclosures per factory specifications. Fusion splices may not be done on ABF fiber bundles.

Electronic files or a CD containing the test results shall be used to verify the fiber optic testing. The test results will be turned-in to the "Office of Enterprise Technology" at final acceptance of the completed project, along with as-built drawings and other required documentation. Any strands that failed shall be repaired or replaced and re-tested.

For major projects, a designated individual from the Communication Installation Vendor shall work with the Panduit, Leviton or Sumitomo factory representatives to obtain the Warranty as part of the close out documentation. This should be completed within 60 days of the completion of the project. An e-mail shall be sent to the manufacturer or vendor representative to schedule a walk-through. The Maricopa County OET Project Manager and designated Lead Technician shall be copied on the e-mail request.

All Sumitomo Tube Cell and Fiber Bundle installations shall be documented and tested. Each cell tube number and the location it is going too shall be documented on an as-built drawing. The tube pressure and obstruction test results shall be recorded once the installation has been completed. This documentation should be done according to the warranty requirements of the manufacturer responsible for issuing the warranty.

Fiber bundle test results for each strand shall be provided in the format required by the manufacturer responsible for issuing the warranty.

SECTION 5: Deliverables

As-Built Drawings

Upon completion of a project, it is required that the Contractor's Lead Technician provide/return to Maricopa County Telecommunications Department/Office of Enterprise Technology, all floor plans or drawings related to the project showing the following information at a minimum:

- a. Horizontal cable routes for drops and tube cell cable, or non-ABF fiber.
- b. Vertical cable routes for feeder cable, tube cell cable, or non-ABF Fiber.
- c. Office drop locations with drop numbers per labeling standards provided in Section One.
- d. ER/TR details showing location and layout of termination blocks.
- e. Locations of vertical conduits or between floor vertical accesses.
- f. Locations and size of horizontal conduits and junction boxes if home run conduits are used for containment of network cabling.

- g. Labeling and placement of Sumitomo ABF TDU, clear tube runs and LIUs.
- h. Locations of ground wire and bus bar(s).
- i. Service provider entrance to building.
- j. Notation of vendor product used for Layer 1 installation (Panduit, Leviton) and fiber installations.
- k. Additional information specific to the installation may be required by the Maricopa County OET Project Manager.

As-built drawings shall be submitted in electronic format using CAD software in DWG file format. Hard copies shall be available upon request.

Test Results

Test results shall be provided in a readable electronic format for all cable runs and fiber installations.

Test results in the format required for the warranty shall be provided for the Sumitomo tube cell cable pressure test; obstruction test and fiber bundle test. A copy of the test results shall be included as part of the deliverables provided to MC-OET.

Warranty

For major projects, a designated individual from The Communication Installation Vendor shall work with the Panduit, Leviton or Sumitomo factory representatives to obtain the Warranty as part of the close-out documentation. This should be completed within 60 days of the completion of the project. An email shall be sent to the manufacturer or vendor representative to schedule a walk-through. The Maricopa County OET Project Manager and designated Lead Technician shall be copied on the e-mail request.

All locations where communications cabling must penetrate floors, firewalls or drywall above the ceiling grid shall be sleeved and fire sealed using an approved firestop system.

11. PINNING.

- b. T568B pinning standard will be utilized on all copper cable terminations.

SECTION 6: Parts List

Cabling material from two (2) manufacturers (Leviton and Panduit) are utilized in the current campus infrastructure for Maricopa County. A list of commonly used parts is shown below. Items not listed require written MC-OET approval prior to installation.

PANDUIT

VENDOR	Part #	DESCRIPTION
PANDUIT	CFPL2EIY	FACEPLATE, SG 2 PORT
PANDUIT	CFPL4EIY	FACEPLATE, SG 4 PORT
PANDUIT	CJ688TGRD	RJ45, CAT6 INSERT – RED
PANDUIT	CJ66UEIY	C3 USOC INSERT – ELECTRIC IVORY
PANDUIT	CMBBL-X	INSERT BLANK BLK
PANDUIT	CMBEI-X	INSERT BLANK EIV
PANDUIT	CMWB	WATERFALL BASE-LADDER RACK

PANDUIT	CMRPSH20	20 AMP HORIZONTAL POWER STRIP
PANDUIT	CMRPSH15	15 AMP HORIZONTAL POWER STRIP
PANDUIT	PRD8	DUAL HINGED METAL DOOR
PANDUIT	PRV8	8"WX84", VERT FRONT REAR MGR
PANDUIT	UICMPP48BLY	48P FLAT MODULAR C6 PATCH PANEL
PANDUIT	UICMPPA48BLY	48P ANGELED MODULAR C6 PATCH PANEL
PANDUIT	NCMHF2	2 RU FRONT ONLY HORIZONTAL CABLE MANAGER
PANDUIT	NCMHAEF2	HORIZONTAL WIRE MGR 2RU HINGED DOOR (PASS THRU's)
PANDUIT	NCMHAEF4	HORIZONTAL WIRE MGR 4RU HINGED DOOR (PASS THRU's)
PANDUIT	DP485E88TGY	FLAT CAT5e 48 PORT PATCH PANEL 110 PUNCHDOWN
PANDUIT	KWP5EY	WALL PHONE JACK AND PLATE
PANDUIT	FAP6WAQDLC	FAP (6) AQUA LC DUPLEX (10GIG)-Terminates 12 fibers
PANDUIT	FAP6WEIDL	FO ADAPTER PANEL 6PACK W MM LC Duplex EIV COUPLERS
PANDUIT	FAP6WBUDLCZ	FO ADAPTER PANEL 6PACK W SM LC
PANDUIT	FLCSMEIY	50 MICRON LC CONN-FLD POLISH
PANDUIT	FLCSSBUY	LC SM CERAMIC ANAEROBIC
PANDUIT	FCE1U	1RU FIBER ENCLOSURE-Holds 4 modules or panels
PANDUIT	FCE4U	4RU FIBER ENCLOSURE-Holds 12 modules or panels
PANDUIT	P110KB1004Y	110 BLOCK 100 PR 4PR - CAT5E KIT
PANDUIT	P110KB1005Y	110 BLOCK 100 PR 5PR - CAT5E KIT
PANDUIT	P110JTW-X	JUMPER TROUGH WITH LEGS
PANDUIT	P110KT3005Y	110 BLOCKI 300PR TOWER
PANDUIT	P110KT9005Y	110 BLOCK 900PR TOWER
PANDUIT	P110JT-X	JUMPER TROUGH WITHOUT LEGS
PANDUIT	P110B100-X	110 BLOCK 100 PR W/O LEGS FOR TOWER
PANDUIT	P110CB4-XY	C4 CLIPS - 10/PKG
PANDUIT	P110CB5-XY	C5 CLIPS - 10/PKG
PANDUIT	PLT2S-M	7 1/2 CABLE TIES
PANDUIT	PLT3S-M	11 1/2" CABLE TIES
PANDUIT	PLT4S-M	14 1/2" CABLE TIES
PANDUIT	JBX3510EI-A	JUNCT BOX BASE/COVER
PANDUIT	LD5EI6-A	6' ELECTRICAL IVORY SURFACE RACEWAY
PANDUIT	CF5EI-E	COUPLER FITTING
PANDUIT	RAF5EI-E	RIGHT ANGLE FITTING
PANDUIT	ICF5EI-E	INSIDE CORNER FITTING
PANDUIT	OCF5EI-E	OUTSIDE CORNER FITTING
PANDUIT	TF5EI-E	TEE FITTING
PANDUIT	ECF5EI-E	END CAP
PANDUIT	DCF5EI-X	DROP CEILING FITTING
PANDUIT	LD10EI6-A	6' ELECTRICAL IVORY SURFACE RACEWAY
PANDUIT	CF10EI-X	COUPLER FITTING
PANDUIT	RAF10EI-X	RIGHT ANGLE FITTING
PANDUIT	ICF10EI-X	INSIDE CORNER FITTING
PANDUIT	OCF10EI-X	OUTSIDE CORNER FITTING
PANDUIT	TF10EI-X	TEE FITTING
PANDUIT	ECF10EI-X	END CAP
PANDUIT	DCF10EI-X	DROP CEILING FITTING

PANDUIT	S100X150YIJ	LAMINATED YELLOW LABELS (2500/PKG)
50M MM FIBER JUMPERS		
PANDUIT	F5D3-3M1Y	1M 50 MICRON SC-SC FIBER JUMPER
PANDUIT	F5D3-3M10Y	10M 50 MICRON SC-SC FIBER JUMPER
PANDUIT	F5D3-3M2Y	2M 50 MICRON SC-SC FIBER JUMPER
PANDUIT	F5D3-3M3Y	3M 50 MICRON SC-SC FIBER JUMPER
PANDUIT	F5D3-3M5Y	5M 50 MICRON SC-SC FIBER JUMPER
PANDUIT	F5D3-3M7Y	7M 50 MICRON SC-SC FIBER JUMPER
PANDUIT	F5E3-10M1Y	1M 50 MICRON SC-LC FIBER JUMPER
PANDUIT	F5E3-10M10Y	10M 50 MICRON SC-LC FIBER JUMPER
PANDUIT	F5E3-10M2Y	2M 50 MICRON SC-LC FIBER JUMPER
PANDUIT	F5E3-10M3Y	3M 50 MICRON SC-LC FIBER JUMPER
PANDUIT	F5E3-10M5Y	5M 50 MICRON SC-LC FIBER JUMPER
PANDUIT	F5E3-10M7Y	7M 50 MICRON SC-LC FIBER JUMPER
PANDUIT	F5F10-10M1Y	1M 50 MICRON LC-LC FIBER JUMPER
PANDUIT	F5F10-10M10Y	10M 50 MICRON LC-LC FIBER JUMPER
PANDUIT	F5F10-10M2Y	2M 50 MICRON LC-LC FIBER JUMPER
PANDUIT	F5F10-10M3Y	3M 50 MICRON LC-LC FIBER JUMPER
PANDUIT	F5F10-10M5Y	5M 50 MICRON LC-LC FIBER JUMPER
50M MM 10GIG FIBER JUMPERS		
PANDUIT	FXE3-10M2Y	2M 50M MM AQUA SC TO LC FIBER JUMPER
PANDUIT	FXE3-10M3Y	3M 50 MM AQUA SC TO LC FIBER JUMPER
PANDUIT	FXE3-10M5Y	5M 50 MM AQUA SC TO LC FIBER JUMPER
PANDUIT	FXE3-10M7Y	7M 50 MM AQUA SC TO LC FIBER JUMPER
PANDUIT	FXE3-10M10Y	10M 50 MM AQUA SC TO LC FIBER JUMPER
PANDUIT	FXE10-10M2Y	2M 50M MM Aqua LC to LC FIBER JUMPER
PANDUIT	FXE10-10M3Y	3M 50M MM Aqua LC to LC FIBER JUMPER
PANDUIT	FXE10-10M5Y	5M 50M MM Aqua LC to LC FIBER JUMPER
PANDUIT	FXE10-10M7Y	7M 50M MM Aqua LC to LC FIBER JUMPER
PANDUIT	FXE10-10M10Y	10M 50M MM Aqua LC to LC FIBER JUMPER
SINGLE MODE		
PANDUIT	F9E3-10M2Y	2M Single Mode SC to LC FIBER JUMPER
PANDUIT	F9E3-10M3Y	3M Single Mode SC to LC FIBER JUMPER
PANDUIT	F9E3-10M5Y	5M Single Mode SC to LC FIBER JUMPER
PANDUIT	F9E3-10M7Y	7M Single Mode SC to LC FIBER JUMPER
PANDUIT	F9E3-10M10Y	10M Single Mode SC to LC FIBER JUMPER
PANDUIT	F9E10-10M2Y	2M Single Mode LC to LC FIBER JUMPER
PANDUIT	F9E10-10M3Y	3M Single Mode LC to LC FIBER JUMPER
PANDUIT	F9E10-10M5Y	5M Single Mode LC to LC FIBER JUMPER
PANDUIT	F9E10-10M7Y	7M Single Mode LC to LC FIBER JUMPER
PANDUIT	F9E10-10M10Y	10M Single Mode LC to LC FIBER JUMPER
COPPER PATCH CABLES – all patch cables should be ordered WITHOUT Boots!		

PANDUIT	UTPSP8BLY	8' C6 BLACK PATCH CORD
PANDUIT	UTPSP10BLY	10' C6 BLACK PATCH CORD
PANDUIT	UTPSP8GRY	8' C6 GREEN PATCH CORD
PANDUIT	UTPSP10GRY	10' C6 GREEN PATCH CORD
PANDUIT	UTPSP15GRY	15' C6 GREEN PATCH CORD
PANDUIT	UTPSP20GRY	20' C6 GREEN PATCH CORD
PANDUIT	UTPSP7YLY	7' C6 YELLOW PATCH CORD
PANDUIT	UTPSP10YLY	10' C6 YELLOW PATCH CORD
PANDUIT	UTPSP15YLY	15' C6 YELLOW PATCH CORD
PANDUIT	UTPSP20YLY	20' C6 YELLOW PATCH CORD
PANDUIT	UTPSP25YLY	25' C6 YELLOW PATCH CORD
PANDUIT	UTPSP7Y	7' C6 WHITE PATCH CORD
PANDUIT	UTPSP10Y	10' C6 WHITE PATCH CORD
PANDUIT	UTPSP15Y	15' C6 WHITE PATCH CORD
SUMITOMO ABF		
SUMITOMO	BE03DW	BLACK DRIVE WHEELS-SET
SUMITOMO	BE03SL	BLACK RUBBER AIR SEAL
SUMITOMO	BE3MFT	BLACK BLOWING TIP THREADED
SUMITOMO	BEBB01	TEST BEADS 100 COUNT – 5MM
SUMITOMO	BEBB40P	TEST BEADS 100 COUNT – 4MM
SUMITOMO	DE20IDU	ABF ENCLOSURE 20HX20WX7D
SUMITOMO	DE08MA	GRAY QR END CAP 10 PK
SUMITOMO	DE08MB	BRASS BULKHEAD QR COUP
SUMITOMO	DE06MP	ORANGE TUBE PLUGS 10/PK - 6MM
SUMITOMO	DE08MC2	CLEAR PLASTIC QR COUPL
SUMITOMO	DE08MT	BLACK T-COUPLING
SUMITOMO	DETC008	TUBE CLIP ORGANIZER
SUMITOMO	DETCB	ABF TUBE ORGANIZER
SUMITOMO	FT3MFB	RUBBER FIBER BUSHINGS – tube plugs
SUMITOMO	BETC001	TUBE CUTTER
SUMITOMO	BETC00B	REPLACEMENT BLADE FOR ABOVE CUTTER
SUMITOMO	FB18SX	18 STRAND SINGLE MODE FIBER
SUMITOMO	FB24SX	24 STRAND SM FIBER
SUMITOMO	FB18M5	18 STRAND MM 50M FIBER (STANDARD)
SUMITOMO	FB18G53	18 STRAND MM 50M FIBER (LASER OPTIMIZED)
SUMITOMO	FB24G53	24 STRAND MM 50M FIBER (LASER OPTIMIZED)
SUMITOMO	FB24M5	24 STR 50 MICRON FIBER (STANDARD)
SUMITOMO	FTFLD18	18-FIBER BUNDLE BREAKOUT KIT
SUMITOMO	FTFLD24	24-FIBER BUNDLE BREAKOUT KIT
SUMITOMO	TC01TXX	TRANSLUCENT TUBE-NON FLAME
SUMITOMO	TC07TP2	7T OFNP 1JKT PLENUM RATED TUBE (1.0 OD)
SUMITOMO	TC19TP2	19T OFNP 1JKT PLENUM RATED TUBES (1.7 OD)
SUMITOMO	TC07TR3	7T OFNR 2 JKT RISER (1.3 OD)
SUMITOMO	TC19TR3	19T OFNR 2JKT RISER (1.9 OD)

Dust-Tight Kellems Strain Relief Grips (for liquid tight – consult SEL specs)		
HUBBELL	73031211	STRAIN RELIEF DELUXE CORD GRIP 1.0 OD (Plenum 7 tube)
HUBBELL	73031212	DELUXE CORD GRIP 1.3 OD (Riser 7 tube)
HUBBELL	73031214	DELUXE CORD GRIP 1.7 OD (Plenum 19 tube)
HUBBELL	73031214	DELUXE CORD GRIP 1.9 OD (for riser 19 tube)
FIBER SUPPLIES		
SYMx	700006737	8.5x11" Type A Brown FO Polish paper w foam back (100PK)
SYMx	700006711	8.5x11" Type D Green FO Polish paper (100Pk)
FISA	680	FO Adhesive Anaerobic Bottle (ea)
FISA	7649	FO Primer Bottle (ea)

LEVITON

VENDOR	VENDOR PART #	DESCRIPTION
LEVITON	49255-H24	24 PORT FLAT PATCH PANEL
LEVITON	49255-H48	48 PORT FLAT PATCH PANEL
LEVITON	49256-H48	48 PORT ANGLED PATCH PANEL - EMPTY
PANDUIT	SRB19BLY	19" STRAIN RELIEF BAR – BLACK (Need 2 for 48 port patch panels)
LEVITON	5500-192	20 AMP HORIZONTAL POWER STRIP NEMA 5-20P INPUT PLUG – NEMA 5-20R RECEPTICLES
LEVITON	5500-190	15 AMP HORIZONTAL POWER STRIP NEMA 5-15P INPUT PLUG – NEMA 5-15R RECEPTICLES
LEVITON	42080-2IS	SINGLE GANG 2 PORT FACEPLATE IVORY – W ID WINDOW
LEVITON	42080-4IS	SINGLE GANG 4 PORT FACEPLATE IVORY – W ID WINDOW
LEVITON	61110-RR6	DARK RED CAT6 SINGLE JACK
LEVITON	61110-BR6	DARK RED CAT6 BULK PACKAGE – 25 – purchase when require multiples of 25 for quantity
LEVITON	41108-RI3	CAT3 USOC IVORY JACK
LEVITON	41084-BEB	BLANK INSERT – BLACK
LEVITON	41084-BIB	BLANK INSERT – IVORY
LEVITON	5F100-12A	6-PACK DUPLEX LC MM (12 fiber) 10 GIG AQUA, ZIRCONIA CERMIC SLEEVE
LEVITON	5F100-12P	6-PACK DUPLEX LC MM (12 fiber) IVORY, PHOSPHORUS BRONZE SLEEVE
LEVITON	5F100-12Z	6-PACK DUPLEX LC SM (12 fiber) BLUE, ZIRCONIA CERMIC SLEEVE
LEVITON	5R2UH-S06	OPT-X ULTRA 2RU FIBER ENCLOSURE (holds 6 plates)
LEVITON	5R4UH-S12	OPT-X ULTRA 4RU FIBER ENCLOSURE (holds 12 plates)
LEVITON	49990-MDL	FAST CURE LC CONNECTOR – MM 50 MICRON FIELD POLISH .9 MM BOOT
LEVITON	49990-SDL	FAST CURE LC CONNECTOR – SM FIELD POLISH .9 MM BOOT
FIBER PATCH CABLES – 50M MULTIMODE		
LEVITON	5LDCL-M01	1M 50 MICRON 10GIG SC-LC FIBER JUMPER (Aqua)
LEVITON	5LDCL-M02	2M 50 MICRON 10GIG SC-LC FIBER JUMPER (Aqua)
LEVITON	5LDCL-M03	3M 50 MICRON 10GIG SC-LC FIBER JUMPER (Aqua)
LEVITON	5LDCL-M05	5M 50 MICRON 10GIG SC-LC FIBER JUMPER (Aqua)
LEVITON	5LDCL-M07	7M 50 MICRON 10GIG SC-LC FIBER JUMPER (Aqua) – NOT STANDARD LENGTH
LEVITON	5LDCL-M10	10M 50 MICRON 10GIG SC-LC FIBER JUMPER (Aqua)

LEVITON	5LDLC-M01	1M 50 MICRON AQUA LC-LC FIBER JUMPER (Aqua)
LEVITON	5LDLC-M02	2M 50 MICRON AQUA LC-LC FIBER JUMPER (Aqua)
LEVITON	5LDLC-M03	3M 50 MICRON AQUA LC-LC FIBER JUMPER (Aqua)
LEVITON	5LDLC-M05	5M 50 MICRON AQUA LC-LC FIBER JUMPER (Aqua)
LEVITON	5LDLC-M07	7M 50 MICRON AQUA LC-LC FIBER JUMPER (Aqua) - NOT STANDARD LENGTH
LEVITON	5LDLC-M10	10M 50 MICRON AQUA LC-LC FIBER JUMPER (Aqua)
LEVITON	5LDSC-M01	1M 50 MICRON AQUA SC-SC FIBER JUMPER (Aqua)
LEVITON	5LDSC-M02	2M 50 MICRON AQUA SC-SC FIBER JUMPER (Aqua)
LEVITON	5LDSC-M03	3M 50 MICRON AQUA SC-SC FIBER JUMPER (Aqua)
LEVITON	5LDSC-M05	5M 50 MICRON AQUA SC-SC FIBER JUMPER (Aqua)
LEVITON	5LDSC-M07	7M 50 MICRON AQUA SC-SC FIBER JUMPER (Aqua) - NOT STANDARD LENGTH
LEVITON	5LDSC-M10	10M 50 MICRON AQUA SC-SC FIBER JUMPER (Aqua)
SINGLE MODE		
LEVITON	UPDCL-S01	1M SINGLE MODE SC-LC FIBER JUMPER
LEVITON	UPDCL-S02	2M SINGLE MODE SC-LC FIBER JUMPER
LEVITON	UPDCL-S03	3M SINGLE MODE SC-LC FIBER JUMPER
LEVITON	UPDCL-S05	5M SINGLE MODE SC-LC FIBER JUMPER
LEVITON	UPDCL-S07	7M SINGLE MODE SC-LC FIBER JUMPER- NOT STANDARD LENGTH
LEVITON	UPDCL-S10	10M SINGLE MODE SC-LC FIBER JUMPER
LEVITON	UPDLC-S01	1M SINGLE MODE LC-LC FIBER JUMPER
LEVITON	UPDLC-S02	2M SINGLE MODE LC-LC FIBER JUMPER
LEVITON	UPDLC-S03	3M SINGLE MODE LC-LC FIBER JUMPER
LEVITON	UPDLC-S05	5M SINGLE MODE LC-LC FIBER JUMPER
LEVITON	UPDLC-S07	7M SINGLE MODE LC-LC FIBER JUMPER- NOT STANDARD LENGTH
LEVITON	UPDLC-S10	10M SINGLE MODE LC-LC FIBER JUMPER
LEVITON	UPDSC-S01	1M SINGLE MODE SC-SC FIBER JUMPER
LEVITON	UPDSC-S02	2M SINGLE MODE SC-SC FIBER JUMPER
LEVITON	UPDSC-S03	3M SINGLE MODE SC-SC FIBER JUMPER
LEVITON	UPDSC-S05	5M SINGLE MODE SC-SC FIBER JUMPER
LEVITON	UPDSC-S07	7M SINGLE MODE SC-SC FIBER JUMPER- NOT STANDARD LENGTH
LEVITON	UPDSC-S10	10M SINGLE MODE SC-SC FIBER JUMPER
COPPER PATCH CABLES – all patch cables shall be ordered with NO Boots!		
LEVITON	6D460-05W	5' CAT6 WHITE PATCH CORD – NO BOOTS
LEVITON	6D460-07W	7' CAT6 WHITE PATCH CORD – NO BOOTS
LEVITON	6D460-10W	10' CAT6 WHITE PATCH CORD – NO BOOTS
LEVITON	6D460-15W	15' CAT6 WHITE PATCH CORD – NO BOOTS
LEVITON	6D460-20W	20' CAT6 WHITE PATCH CORD – NO BOOTS
LEVITON	6D460-05Y	5' CAT6 YELLOW PATCH CORD – NO BOOTS
LEVITON	6D460-07Y	7' CAT6 YELLOW PATCH CORD – NO BOOTS
LEVITON	6D460-10Y	10' CAT6 YELLOW PATCH CORD – NO BOOTS
LEVITON	6D460-15Y	15' CAT6 YELLOW PATCH CORD – NO BOOTS
LEVITON	6D460-20Y	20' CAT6 YELLOW PATCH CORD – NO BOOTS
LEVITON	6D460-05G	5' CAT6 GREEN PATCH CORD – NO BOOTS
LEVITON	6D460-07G	7' CAT6 GREEN PATCH CORD – NO BOOTS

LEVITON	6D460-10G	10' CAT6 GREEN PATCH CORD – NO BOOTS
LEVITON	6D460-15G	15' CAT6 GREEN PATCH CORD – NO BOOTS
LEVITON	6D460-20G	20' CAT6 GREEN PATCH CORD – NO BOOTS
LEVITON	6D460-07E	7' CAT6 BLACK PATCH CORD – NO BOOTS
LEVITON	6D460-10E	10' CAT6 BLACK PATCH CORD – NO BOOTS
LEVITON	6D460-15E	15' CAT6 BLACK PATCH CORD – NO BOOTS
LEVITON	6D460-20E	20' CAT6 BLACK PATCH CORD – NO BOOTS
LEVITON	41AB2-1F4	110 Block 100 Pr w legs - 5e C4 Kit
LEVITON	41AB2-1F5	110 Block 100 Pr w legs - 5e C5 Kit
LEVITON	41MB2-3F4	110 BLOCK 300PR TOWER
LEVITON	41A10-HCM	110 JUMPER TROUGH W/LEGS

CPI

VENDOR	VENDOR PART #	DESCRIPTION
CPI	55053-703	19"X7' STANDARD RACK - BLACK
CPI	10595-712	BLACK 12" RACK MOUNTING PLATE
CPI	11421-712	WALL ANGLE SUPPORT KIT FOR 12" LADDER - BLACK
CPI	10610-019	19"RACK HORIZONTAL BUSBAR
CPI	10250-712	12" UNIVERSAL CABLE RUNWAY-BLACK
CPI	10642-001	END CAP 1.5X3/8 BLACK
CPI	11301-001	BUTT-SPLICE KIT - GOLD
CPI	11302-001	JUNCTION SPLICE – 90 DEGREE - GOLD
CPI	11312-712	BLACK 12" TRIANGULAR SUPPORT BRACKET
CPI	12833-703	GLOBAL SINGLE SIDED VERTICAL CABLE MANAGER – BLACK 7'Hx6"Wx9.3"D (need 2 for 1 rack)
CPI	12836-702	CABLE RINGS FOR GVCS – SET OF 7 (Use for back side of vertical cable management)
CPI	12100-706	CABLE RADIUS DROP – FOR CROSS MEMBER ATTACHMENT – 5" WIDE -BLACK
CPI	12101-703	CABLE RADIUS DROP – FOR STRINGER ATTACHMENT – 5" WIDE -BLACK
CPI	40153-012	TMGB – BUSBAR 4"W x 1/4"H x 12"L (Used in ER (MDFs)
CPI	13622-012	TGB – BUSBAR 2"W x 1/4"H x 12"L (Used in TC (IDFs)
CPI	30130-719	19" 2RU 5" DEEP HORIZONTAL CABLE MANAGER – SINGLE SIDED - BLACK
CPI	TS1004331	19" SINGLE SIDED BLACK 4 RU HORIZONTAL CABLE MANAGER

MISCELLANEOUS PARTS

VENDOR	VENDOR PART #	DESCRIPTION
3M	80610551105	ELECTRICAL TAPE
3M	98040054177	FIREPUTTY
HILTI	378287	2" FIRE BARRIER MUFFIN
HILTI	378288	4" FIRE BARRIER MUFFIN
STI	EZDP33FWS	FIRE BARRIER SLEEVE
B-Line	BCH32-W2	2" J HOOK
GARV	PL-230-CSC	BUCKET OF 6500# JETLINE

CADDY	MPLS	METAL SINGLE GANG MOUNTING PLATE BRACKET W DRYWALL SCREWS
	189645	25 YARD ROLL VELCRO
AMIN	12590	6 GA STRANDED GREEN GROUNDING WIRE
BURNDY	YA6CL2	2 HOLE GROUND LUGS
CIRCA	1880ENA1/NSC-12	12/PR PROTECTOR 110 STYLE
CIRCA	1880ENA1-NSC-25	25/PR PROTECTOR 110 STYLE
CIRCA	1880ENA1-NSC-50	50/PR PROTECTOR 110 STYLE
CIRCA	1880ENA1-NSC-100	100/PR PROTECTOR 110 STYLE
CIRCA	3B1E	GAS MODULES
Boxed Cable (1000')		
SUPERIOR	66-246-4B	4 PR 23 AWG CAT6 CABLE - CMP WHITE
SUPERIOR	18-241-46	4 PR 24AWG CAT3 CABLE - CMP WHITE
GENERAL	7131901	4 PR 23AWG CAT6 CABLE - CMP WHITE
GENERAL	2131245	PR 24AWG CAT3 CABLE - CMP WHITE

PARTS LIST FOR DATA CENTER BUILDOUT – Downtown and Disaster Recovery Site

VENDOR	VENDOR PART #	DESCRIPTION
PANDUIT	CRS4-125-X	STACKABLE CABLE RACK SPACERS
PANDUIT	DPFP1	BLANK PANEL FILLER 1 RU 19"
PANDUIT	DPFP2	BLANK PANEL FILLER 2 RU 19"
PANDUIT	DPFP4	BLANK PANEL FILLER 4 RU 19"
PANDUIT	FRBC6X4YL	YELLOW 6X4 COUPLER
PANDUIT	FREC6X4YL	END FITTING 6X4 YELLOW
PANDUIT	FRFWCSC6YL	SPLT COVER FOR 4-WAY HORIZ YELLOW
PANDUIT	FRFWC6X4YL	4-WAY CROSS FITTING 6X4
PANDUIT	FRRASC6YL	SPLIT COVER FOR RIGHT ANGLE (90 Degree) FITTING YELLOW
PANDUIT	FRRAC6X4YL	RIGHT ANGLE (90 Degree) FITTING 6X4 YELLOW
PANDUIT	FRHC6YL6	DUCT COVER 6X4 6' YELLOW
PANDUIT	FRT6X4YL	HORIZONTAL TEE 6X4 YELLOW
PANDUIT	FRTSC6X4YL	SPLIT COVER FOR HORIZONTAL TEE 6X4 YELLOW
PANDUIT	FRVT6X4YL	TEE 6" VERT YELLOW
PANDUIT	FR6ALB	LADDER BRACKET 6" ADJUSTABLE – FOR TROUGH
PANDUIT	FR6X4YL6	DUCT SOLID 6X4 6' YELLOW TROUGH (6' lengths)
PANDUIT	FRHC6YL6	SNAP-ON HINGED COVER FOR TROUGH (6' lengths)
PANDUIT	FR6TRBN58	Quick Lock Bracket for 5/8 all thread (used at DR site for Translucent tube support)
LEVITON	6D460-50L	50' CAT6 SOLID CMR PATCH CORD WITH MODULAR PLUG AND NO BOOTS (use for cross connect)
PANDUIT	UPBU50Y	C6 SOLID CMR W/TX6 MOD PLUG (data center- USE ONLY)
CPI	TS1004331	4RU UNIVERSAL HORIZONTAL CABLE MANAGER 19" WIDE – HINGED SNAP-ON COVER - BLACK
LEVITON	49254-BP1	1RU BLANK FILLER PANEL – 19" BLACK
LEVITON	49254-BP2	2RU BLANK FILLER PANEL – 19" BLACK
LEVITON	49254-BP4	4RU BLANK FILLER PANEL – 19" BLACK

LEVITON	34537-000	SNAP IN FILLER PANEL 1U 1 PC (server cabinets only – cage nut rails)
LEVITON	34537-001	SNAP IN FILLER PANEL 1U 6 PC (server cabinets only – cage nut rails)
LEVITON	34538-000	SNAP IN FILLER PANEL 2U 1 PC (server cabinets only – cage nut rails)
LEVITON	34538-001	SNAP IN FILLER PANEL 2U 6PC (server cabinets only – cage nut rails)
CPI	55053-703	19"X7' DISTRIBUTION RACK
CPI	TS1005742	T2 CABINET FOR HIGH DENSITY SERVERS – BLACK
CPI	TS1005701	T2 CABINET FOR HOT/COLD AISLE – SERVERS – BLACK
CPI	34434-C01	PDU MOUNTING BRACKET FOR 6509 SWITCH CABINETS – need purchase 1 additional for mounting second power strip in each cabinet
CPI	10596-708	CABLE RETAINING POST – 8" HIGH BLACK W END CAPS – use for cable row management
CPI	10250-724	24" LADDER TRAY - BLACK
CPI	11421-724	24" WALL ANGLE SUPPORT KIT - BLACK
CPI	13392-712	PATH DIVIDER FOR LADDER TRAY – BLACK
CPI	DP3082364	6509 Switch Cabinet with cable Management fingers/exhaust duct (for DR site)
CPI	34434-C01	Power strip mounting bracket (need to order one for each cabinet – if use APC 7983 PDU)

Note: Vertical cable management for the racks will be determined by the Maricopa County OET Project Manager at the time of purchase.

SECTION 7: References

- a. Design, manufacture, test, and install per manufacturer's requirements, the standards referenced herein, in accordance with NFPA-70 (National Electrical Code®) based on the version adopted by the authorities having jurisdiction (AHJ), IEEE C2 2007(NESC 2007), state codes, local codes, and the requirements of the AHJ. Please note that NEC® is intended to protect property and people from electrical hazards and do not necessarily address requirements for the reliable and error free operation of electrical systems. Additional requirements exceeding the safety provisions of NEC® may be required to ensure the expected performance of specific systems.
 1. ANSI/NECA/BICSI-568-2006 -- Standard for Installing Commercial Building Telecommunications Cabling
 2. ANSI/BICSI 002-2011, Data Center Design and Implementation Best Practices.
 3. ANSI/TIA-568-C.0 – Generic Telecommunications Cabling for Customer Premises
 4. ANSI/TIA-568-C.0-1-2010 – Generic Telecommunications Cabling for Customer Premises-Addendum 1, Updated References for Balanced Twisted-Pair
 5. ANSI/TIA-568-C.1-2009 – Commercial Building Telecommunications Cabling Standard
 6. ANSI/TIA-568-C.2-2009 – Balanced Twisted-Pair Telecommunications Cabling and Component Standard
 7. ANSI/TIA/EIA-568-C.3-2009 -- Optical Fiber Cabling Components Standard
 8. ANSI/TIA/EIA-569-B-2004 -- Commercial Building Standard for Telecommunications Pathways and Spaces
 9. ANSI/TIA/EIA-569-C-2005—Optical Fiber Cable Color Coding
 10. ANSI/TIA/EIA-606-A-2002 -- The Administration Standard for Commercial Telecommunications Infrastructure
 11. ANSI/J-STD-607-A -- Commercial Building Grounding and Bonding Requirements for Telecommunications
 12. ANSI-J-STD-607-B-2011 -- Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications
 13. TIA-526-14B-2010 –OFSTP-14 Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant

14. ANSI/TIA/EIA-758-B-2011 -- Customer-Owned Outside Plant Telecommunications Infrastructure Standard
15. ANSI/TIA/EIA-862-A-2011, Building Automation Systems Cabling Standard
16. ANSI/TIA-942-2005, Telecommunications Infrastructure Standard for Data Centers
17. ANSI/TIA-1152-2009, Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling.
18. NECA/BICSI 607-2011, Standard for Bonding and Grounding Planning and Installation Methods for Commercial Buildings
19. TIA TSB-140 Additional Guidelines for Field Testing Length, Loss And Polarity of Optical Fiber Cabling Systems
20. Install cabling in accordance with the most recent edition of BICSI® publications:
21. BICSI– Telecommunications Distribution Methods Manual-12th Edition
22. BICSI– Information Technology Systems Installation Methods Manual, 6th Edition
23. BICSI – Installation Transport Systems Information Manual
24. BICSI –Outside Plant Design Reference Manual-5th Edition
25. BICSI – Wireless Design Reference Manual-3rd Edition
26. BICSI – AV Design Reference Manual-1st Edition
27. InfoComm International- ANSI/INFOCOMM 2M-2010, Standard Guide for Audiovisual Systems Design and Coordination Processes
28. BICSI– Network Design Reference Manual- 7th Edition
29. The Americans with Disabilities Act (ADA) of 1992 Title IV: Telecommunications of the Telecommunications Act, Section 4.31: Telephones of the Americans with Disabilities Act (ADA) Accessibility Guidelines (ADAAG). "Accessibility Guidelines for Buildings and Facilities", and Section 255
30. NFPA 1221, Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems 2010 Edition.

EXHIBIT J**IMPLEMENTATION SCHEDULE**

As soon as practical after Contract initiation, the Parties shall determine the appropriate course of action for implementation of VVS. The optimal plans are outlined below. A full formal schedule shall be produced with deliverables and delivery dates.

1. Start with the jails that currently have "contact" visitation Durango, Estrella, and/or Towers. Install systems in the pods/visitation lobbies. Continue with "contact" visitations until Durango Triangle (LBJ, Towers, Durango, and Estrella) system can be turned on. (Durango, Tents, Towers and Estrella can be installed simultaneously or individually)
2. FMD or Sheriff's FMOs will remove plywood boarding from Tents "Non-Contact" windows in visitation lobby and Securus will implement new kiosk in old video visitation area. Tents then will revert back to "Non-Contact" visitation until new system can be turned on at the Durango Triangle.
3. Since the LBJ current system and Securus' new system will not be running parallel; Jail visitation will cease for the amount of time it takes to install the system completely in the jail. Therefore it paramount the system is installed as quickly as possible. When system is completed at LBJ the new Securus system along with the Durango Triangle will go live.
4. Since the 4th Ave's current system and Securus' new system will not be running parallel; Jail visitation will cease for the amount of time it takes to install the system completely in the jail. Therefore it paramount the system is installed as quickly as possible. When system is complete at 4th Ave the new Securus system will then go live.

Or

1. Start with the jails that currently have "contact" visitation Durango, Estrella, and/or Towers. Install systems in the pods/visitation lobbies. Continue with "contact" visitations until Durango Triangle (LBJ, Towers, Durango, and Estrella) system can be turned on. (Durango, Tents, Towers and Estrella can be installed simultaneously or individually)
2. FMD or Sheriff's FMOs will remove plywood boarding from Tents "Non-Contact" windows in visitation lobby and Securus will implement new kiosk in old video visitation area. Tents then will revert back to "Non-Contact" visitation until new system can be turned on at the Durango Triangle.
3. LBJ and 4th Ave systems will be installed concurrently; and since the LBJ and 4th Ave's current system and Securus' new system will not be running parallel; Jail visitation will cease for the amount of time it takes to install the system completely in the jail. Therefore it paramount the system is installed as quickly as possible. When system is completed at LBJ and 4th Ave the new Securus system with Sheriff's Office will go live simultaneously.

EXHIBIT K

HOSTING REQUIREMENTS

1.0 AVAILABILITY:

- 1.1 Any information systems required for proper functionality of the hosted application shall have 99.99% uptime during County business hours. Uptime measurements shall be met for all servers and their connectivity to the Internet or dedicated connection to the County, whichever is applicable.
- 1.2 An industry-recognized backup methodology shall be employed, including the use of off-site storage. The Contractor shall make backup procedures and logs available at any time upon request from the County.
- 1.3 Application response time, defined as the time it takes to complete render the user interface after a user action, shall be less than three (3) seconds. Unacceptable response times shall be considered to make the program unavailable and will count against the 99.99% uptime metric.

2.0 CONNECTIVITY:

- 2.1 The Contractor shall provide connectivity to the Internet or use Virtual Private Networking (VPN), whichever is appropriate. The County shall not be financially responsible for networking equipment at the Contractor site.
- 2.2 Client applications installed on user workstations that shall contact the off-site hosting environment shall be able to do so through an HTTP proxy. Workstations shall not be required to directly connect over the Internet for any reason.

3.0 DATA SECURITY:

- 3.1 Backups to removable media shall be encrypted using the Advanced Encryption Standard (AES) with a minimum of a 128 bit key. Industry recognized key handling procedures shall be utilized. At no time shall the key be stored on the backup media in clear text, including but not limited to table labels. The Contractor shall make key handling procedures and logs available upon request.
- 3.2 Hosted applications shall support encrypted protocols for sensitive data. Preferred encryption protocols are Secure Sockets Layer (SSL) and Internet Protocol Security (IPSec). Encryption ciphers shall use at least a 128 bit key length. Hashing algorithms used shall be of the Secure Hash Algorithm (SHA) family. The minimum acceptable algorithm shall be SHA-1.
- 3.3 All hosted solutions shall be audited by a third party at least once per year. The Contractor shall provide attestation by a 3rd party (e.g. SSAE16 Type 2/SAS 70 Type II) at any time upon the County's request.
- 3.4 All applications hosting Maricopa County data shall undergo a risk assessment at least twice per year. The risk assessment shall include system and application testing. The results shall be made available to the County upon request.
- 3.5 The Contractor shall maintain a non-disclosure agreement (NDA) with the County. All employees of the Contractor shall maintain an NDA with the Contractor.
- 3.6 All employees of the Contractor shall pass a federal, state, and local criminal background check. Any employee who fails the background check shall not have any access to County data unless specifically authorized by Maricopa County in writing. The Contractor shall make personnel and background check procedures available for inspection at any time upon request from the County.

- 3.7 No County data shall be transferred or made available to a 3rd party in unencrypted form without the express, written consent of the County. See the "Backups" section for what shall be considered "encrypted."
- 3.8 No County data shall be transferred or transmitted outside the United States for any reason without the express, written consent of the County.
- 3.9 The system shall support password policy enforcement, such as mixed case, numerals, and non-alphanumeric characters.
- 3.10 The system shall support the ability to disable or lock out user accounts after a given number of login failures.

4.0 INFORMATION SYSTEMS AUDITING:

- 4.1 The system shall log all material user actions, including but not limited to, logon and log off.
- 4.2 The system shall log all material administrator actions, including but not limited to, user creation, user deleting, password resets, and privilege level changes.
- 4.3 The system shall log failed login attempts.
- 4.4 Logs shall be made available to the County at any time.

5.0 BREACH NOTIFICATION:

- 5.1 The Contractor shall report all suspected breaches to the County immediately and in writing. The Contractor shall also fully cooperate with any County investigation into the breach, unless prohibited by law.
- 5.2 Should a breach of the hosted service occur, the Contractor shall bear the full cost of breach notification and any follow-up services. Follow-up services include, but are not limited to, credit monitoring of affected individuals.
- 5.3 Should a breach of the hosted service occur, the Contractor shall pay all fines associated with the breach.
- 5.4 Breach notification requirements shall be determined by all applicable laws and contracts including, but not limited to, Arizona Revised Statutes 44-7501, California SB 1386, the Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI).
- 5.5 The Contractor shall make the information security incident response policy and procedure available to the County at any time upon request.

6.0 COMPLIANCE:

- 6.1 The Contractor shall comply with all applicable laws, regulations, and contracts including (but not limited to) Criminal Justice Information Systems (CJIS), Health Insurance Portability and Accountability Act, and Payment Card Industry (PCI).
- 6.2 The Contractor shall make compliance reports, audit findings, and 3rd party attestations available at any time to the County upon request.
The Contractor shall immediately notify the County, in writing, upon a confirmed violation of the compliance requirement. The notification shall include any information provided by the regulatory body.
- 6.3 Contractors that host applications containing HIPAA protected data shall enter into a Business Associate agreement (as defined by HIPAA) with the County. The Business Associate agreement shall be maintained for the life of the contract.

7.0 DATA RETENTION:

- 7.1 The Contractor shall destroy all offline copies of County data at the time ceases to be useful. Destruction procedures shall be made available to the County upon request.
- 7.2 At the conclusion of the contract, all Maricopa County data and working papers shall be returned to the County and all Contractor copies destroyed. The Contractor shall confirm in writing to the County that all data was destroyed in accordance with this agreement and state the methodology used.

EXHIBIT L**MINIMUM KIOSK DEPLOYMENT REQUIREMENT****Facility Totals**

Facility	Regular	Vis-Lobby	Roll-a-bouts	Sub-Total	Public/ Legal Booths	Total w/public
4 th Ave	112	-	16	128	38/6	172
LBJ	124	-	12	136	54/8	198
Towers	48	-		48	-	48
Tents	29	-	-	29		29
Durango	96	-	-	96	-	96
Estrella	56	-	3	59	-	59
GRAND TOTALS	465	0	31	496	92/14	602

4th Ave Jail

House	100 Pod	200 Pod	Total
2A	4	4	8
2B	4	4	8
2C	4	4	8
2D	4	4	8
2E	4	4	8
2F	4	4	8
		Sub-Total	48
3A	4	4	8
3B	4	4	8
3C	4	4	8
3D	4	4	8
3E	4	4	8
3F	4	4	8
		Sub-Total	48
4A	4	4	8
4F	4	4	8
		Sub-Total	16
SMU			
Runs 1,2,3,4	roll-a-bouts	roll-a-bouts	-
4B & 4E	roll-a-bouts	roll-a-bouts	16
		I/M Kiosks	112
		Sub-Total	128
		Public Visitor Station	38
		Legal Booths	6
		Total	172

Lower Buckeye Jail

House	Pod A	Pod B	Total
T11	4	4	8
T12	4	4	8
T13	4	4	8
T14	4	4	8
T21	4	4	8

T22	4	4	8
T23	4	4	8
T24	4	4	8
T31	4	4	8
T32	4	4	8
T33	4	4	8
T34	4		
		Sub-Total	96
Dorms	North-side	South-side	
M1	2	2	4
M2	2	2	4
M3	2	2	4
M4	2	2	4
		Sub-Total	16
Psych	Pod A	Pod B	
P1	1	1	-
P2	1	1	-
P3	1	1	-
P4	1	1	-
P5	1	1	-
P6	1	1	-
Add 1 roll-a-bout port	per pod.	Sub-Total	0
		I/M Kiosks	124
Infirmary	roll-a-bouts	roll-a-bouts	12
		Sub-Total	136
		Public Visitor Station	54
		Legal Booths	8
		Total	198

Towers Jail

House	Pod A	Pod B	Pod C	Pod D		Total
T1	2	2	2	2		8
T2	2	2	2	2		8
T3	2	2	2	2		8
T4	2	2	2	2		8
T5	2	2	2	2		8
T6	2	2	2	2		8
					Sub-Total	48
					Vis-lobby	0
				Total		48

Tents Jail

Dorm	N	0	H	Total
Yards	12	10	7	29
			Total	29

Durango Jail

House	Pod A	Pod B	Pod C	Pod D		Total
D1	3	3	3	3		12
D2	3	3	1	3		10
D3	1	3	3	3		10
D4	3	3	3	3		12
D5	3	3	3	3		12
D6	3	3	3	3		12
D7	3	3	3	3		12
					Sub-Total	80
Dorm	Southeast wall					
D8	8					8
D9	8					8
					Sub-Total	16
					Vis-lobby	0
					Total	96

Estrella Jail

House	100 Pod	200 Pod	300 Pod	400 Pod	Total
A	2	2	2	2	8
B	2				2
B (CC)		1 roll-a-bouts	1 roll-a-bouts	1 roll-a-bouts	3
C	2	2	2	2	8
D	2	2	2	2	8
Dorms	Dayroom				
E	4				4
F	4				4
G	4				4
H	INCLUDED	ABOVE	IN	TENTS	
I	4				4
J	4				4
K	4				4
L	4				4
M (JUVY)	1	1			2
				Sub-Total	56
				Roll-a-bouts	3
				Vis-lobby	0
				Total	59

SECURUS TECHNOLOGIES INC., 14651 DALLAS PARKWAY STE 600, DALLAS, TX 75254

PRICING SHEET: NIGP CODE 83834

Vendor Number: 2011003803 0

Certificates of Insurance Required

Contract Period: To cover the period ending **November 30, 2018.**

5.20.1 Table of Contents

5.20.2 Letter of Transmittal.....	1
5.20.3 Executive Summary.....	3
5.20.4 Proposal.....	6
5.20.5 Qualifications.....	149
5.20.6 Proposal Exceptions.....	152
5.20.7 Other Data.....	153
Appendix A: Preliminary Implementation Schedule	
Appendix B: Securus Test and Acceptance Documents and Checklists	
Appendix C: Certificate of Insurance	
Appendix D: Resumes	
Appendix E: Arizona Business Certificates	
5.20.8 Attachment A (Pricing)	162
5.20.9 Attachment B (Agreement Page)	165
5.20.10 Attachment C (References).....	166
5.20.11 Attachment D (Questionnaire).....	167
5.20.12 Exhibit 3, Sole Proprietor Waiver (If applicable).....	182
Addenda Acknowledgements	183
Addendum 1	
Addendum 2	
Addendum 3	
Addendum 4	

5.20.2 Letter of Transmittal

March 22, 2013

Paul Aguilar
Office of Procurement Services
320 West Lincoln Street
Phoenix, Arizona 85003-2494

RE: RFP # PC 13002- Web- Based Visitation/Communication Kiosk System

Dear Paul:

Securus Technologies is excited to submit our proposal in response to RFP #PC 13002 – Web Based Visitation/ Communication Kiosk System. Securus offers your solution for video visitation. Our Video Visitation solution is the best video visitation service in the industry. The Securus video visitation platform delivers features that are not found in any other video visitation systems.

The Securus Video Visitation System (SVV) being proposed to fulfill the requirements of this RFP, is an integrated IP based, real time, corrections based communication system. SVV is a combination of state of the art video conferencing technology, browser based network control and scheduling, enterprise level computing and storage, with the most sophisticated digital recording and monitoring on the market today. By offering a zero cost solution which allows for visitors to visit from home/remotely, it will reduce labor, and automate systems, as it integrates with your current JMS. You will be pleased to know that we have competitively priced the Video Visitation Sessions to ensure that the inmate phone revenues will not be cannibalized by Video Visitation session prices being too low.

With our offer of best in class video visitation through Securus, we believe we can exceed your expectations for the provisions of this invitation to bid. A partnership with Securus will provide Maricopa County with greater revenues, improved security, and improved investigative capabilities with the addition of our unique THREADs™ lead generation product.

Darrin Hays is the Account Manager responsible for Maricopa County's solution presented in our response. He will be your contact to provide answers to any questions that the County may have. Mr. Hays can be contacted by (480) 717-8790 or by email at dhays@securustech.net.

We thank you for your consideration of the attached proposal and look forward to the opportunity of beginning a mutually beneficial relationship with Maricopa County and its constituents as your provider for Remote and On-Site Video Visitation.

Thank you for the opportunity to submit our proposal.

Sincerely,

Robert E. Pickens, Chief Operating Officer
Securus Technologies, Inc.
14651 N. Dallas Parkway, Suite 600
Dallas, Texas 75254
972-277-0300
bpickens@securustech.net

5.20.3 Executive Summary

Thank you for allowing Securus Technologies, Inc. to participate in this opportunity to provide a Video Visitation System to Maricopa County. We have reviewed your requirements and demonstrate in our response that we meet or provide a functional alternative to an overwhelming majority of Maricopa County's requirements.

The Securus Video Visitation (SVV) System is a proven option for Video Visitation and best in class.

Securus leads the inmate telephone industry with more than 25 years of experience, over 2,200 installed facilities, and with approximately 100 patents driving customer-inspired solutions. While we are proud of our heritage, we don't rest on our accomplishments. We continue to re-invest in our people, platforms, and products and have committed over \$17 million in incremental spending over the last year to further our industry-leading capabilities. No competitor can match our level of re-investment or our patented inmate communication technologies. We are committed to continue to lead our industry.

Furthermore, it is our number one goal to bring you solutions to better enhance your facility and staff operations. Your Arizona based team is committed to understand your needs and will work diligently to help you achieve your goals!

The SVV system being proposed is an integrated IP based, real time, detention based communication system. SVV is a combination of state of the art video conferencing technology, browser based network control and scheduling, enterprise level computing and storage, with the most sophisticated digital recording and monitoring on the market today. Each unit will deliver fully integrated detention based technology solution in a single system deployment. These units will offer the following capabilities to meet your needs:

Unmatched Technology – Securus Video Visitation System

Highlights of the video visitation system include:

- Video Visitation
- Remote and completely secure attorney-client communication
- Live Monitoring and Recording
- Long term storage of recorded visitation sessions
- Automated retrieval and playback
- Jail Management system interface
- Browser Based Scheduling and Visitor Registration

- Browser Based System Administration
- Call History Record
- Usage Reporting
- Proven customer service capabilities to ensure community satisfaction

Maximizing Opportunities, Operational and Investigative Needs

Securus understands that every dollar is critical to Maricopa County, so Securus has provided an offer that provides you with the technology you requested. From a review of your proposal components, we have identified that you need:

- The SVV system, which includes the features, functionality, hardware, maintenance, training, and support
- An expedited and seamless installation
- Remote visitation generating commissionable revenue streams and providing additional services to the community
- **Maintenance and support are included free as part of our offer—other providers offer maintenance and support for a FEE**
- **Bandwidth included in our offer—other providers offer bandwidth for a FEE, through a commission deduction, or offer a monthly stipend that generally will not cover the basic expenses of the bandwidth**
- Maximized technology to improve productivity and increase services
- Investigative analytic technology to provide additional data gathering value to visitations
- A vendor that has successful experience and integration experience with other vendors in the commissary and jail management systems
- An experienced and capable provider that knows how to provide superior customer service without sacrificing technology and revenues
- A quality team to work with jail staff on training, how to effectively utilize the system, and work on any main initiatives to improve efficiency of operations through and with the video visitation system
- An advanced system that provides reliability, functionality, ease of use, and total collaboration
- Three On-Site Administrators—or a functional equivalent—who are trained in supporting Securus-designed Video Visitation Systems and kiosk applications

Conclusion

We want to be your chosen partner and hope that we have answered all your questions and provided you the information you need to make your decision.

By choosing Securus you'll get:

5.20.3 Executive Summary

- The Securus Video Visitation System with a multitude of kiosk capabilities
- The leader in terms of experience, capabilities, technology, financial stability, and customer service
- A partner who understands your needs and has the resources and commitment to meet your changing needs in the future
- Revenue sharing from remote visitation sessions without strings for technology and service

We sincerely thank you for this opportunity and look forward to growing a long-term, mutually beneficial relationship with Maricopa County.

5.20.4 Proposal

This section should contain a statement of all of the programs and services proposed, including conclusions and generalized recommendations. Proposals should be all-inclusive, detailing respondent's best offer.

Maricopa County (hereafter referred to as County) requests your organization to submit a written proposal to enter into a revenue contract for providing a completely installed and functioning Internet-based remote video visitation and inmate communication kiosk system. Also, multiple distinct phases providing additional functionality are detailed in this document including: inmate email, ability to access policies and complete basic forms including, but not limited to, Inmate Request Forms, Inmate Grievances, Disciplinary Action Appeals, and Health Needs Request Forms. The system will also provide the ability to order from the MCSO Commissary. This would be an all-inclusive kiosk system that would allow Maricopa County Sheriff's Jails (hereafter referred to as MCSO) to go virtually paperless. The system must allow access from any location with Internet service.

Proposals are solicited to establish a contract for the furnishing, installation, and maintenance of a Web-based Video Visitation/Communication Kiosk System in the Maricopa County Jail facilities and provide the necessary equipment, software and personnel expertise to implement, maintain, reproduce and monitor video recordings of all visits in this contract.

An overview of the current inmate video visitation system and equipment is available in Exhibit 9. The jail population demographics are listed in Exhibit 10.

Other governmental entities under agreement with the County may have access to services provided hereunder (see also Section 4.17 and 4.18, below).

The County reserves the right to add additional contractors, at the County's sole discretion, in cases where the currently listed contractors are of an insufficient number or skill-set to satisfy the County's needs or to ensure adequate competition on any project or task order work.

✓ **Securus has read, understands, and complies.**

Securus Video Visitation (SVV) is available for immediate installation and use by Maricopa County. SVV is a fully Web-based video visitation platform and integrated inmate kiosk solution specifically designed for correctional facilities.

SVV will enable Maricopa County to conduct visitations safely, securely, and with fewer burdens on facility staff. This advanced solution provides multiple benefits, including:

- Enhanced facility security by reducing the possibility of inmate confrontation
- Reduction in inmate and visitor movement through a facility
- Improved inmate ability to communicate with legal representation, bail-bond facilities, family, and any other persons authorized by Maricopa County Jail administration

- Reduction in contraband infiltration
- Increased security for visitors
- Increased inmate and visitor morale with increased opportunities to visit
- Reduced resources needed to escort inmates and visitors to visiting areas
- New revenue stream for the facility through paid visitation sessions

The SVV solution is a centralized system that allows for automatic technology and feature upgrades. After the video visitation system has been implemented, it is easy for Securus to enable new features and modules by activating the feature in the centralized system. SVV will enable inmates to order from the commissary as well as complete inmate requests and grievance forms using the terminal, enabling the Maricopa County Sheriff's Office (MCSO) to work toward its goal of attaining a paperless environment.

At-home or remote visitation sessions allow friends and family, bail bondsmen, probation officers, and attorneys to securely communicate with inmates from outside the facility via a broadband Internet connection. Because SVV is Internet-based, visitation sessions can be scheduled and conducted from any location with Internet services.

Remote visitors access Securus Video Visitation through the www.securustech.net Web site. The visitor selects the facility and inmate they would like to visit. The visitor is able to do the following:

- Create, edit, and/or delete scheduled video sessions with inmates
- Pay for the scheduled session with a credit or debit card
- Visit with inmates (no officer intervention required)

Remote users will need to use a personal computer or laptop with a built-in or external USB Web camera, a microphone and speakers, or a headset.

Securus will provide SVV to Maricopa County, including installation and maintenance as well as personnel to operate and maintain the system.

2.0 SCOPE OF WORK:

2.1 GENERAL REQUIREMENTS

Maricopa County is seeking a single Contractor with end-to-end responsibility for a turnkey inmate Web-based Video Visitation/Communication Kiosk System and services. Subcontractor relationships shall be permitted; however, the Contractor shall be responsible for the entire operation of the Web-based Video Visitation/Communication Kiosk system. The proposer shall verify the completeness of all service components and ensure that any and all equipment, materials and services required for installation, operation, or maintenance will be provided by proposer without claim for payment or reduction in commission level. Maricopa County shall bear no responsibility for any costs associated with the equipment and services solicited in the document. Solutions limited to point to point access will not be considered.

The Web-based Video Visitation/Communication Kiosk system must provide differentiation between legal and personal visits with a check and balance for the specific type of visit being requested, digital recording of personal visits made and a time synched network for all associated equipment in the system. The system must be of an open architecture to allow ease of integration with existing or future systems that operate on either PC based networks or mainframes. It must meet ADA requirements, provide access to both Spanish and English at the minimum, if not more, and have extensive IP address blocking capabilities at various levels and various times as deemed necessary by MCSO. The system shall be capable of downloading data to MCSO applications for investigative and statistical purposes and capable of receiving downloaded data from the Sheriff's Office Jail Management System or other MCSO systems. No third party/conference video chatting is permitted, unless specified by MCSO.

The system shall be an Internet based remote video visitation system and shall include inmate stations [and a limited number of public visiting stations located at LBJ and 4th Avenue Jails] controlled via an Operator Control/Reception Station.

The system shall consist of cameras, monitors, microphones/handsets, audio-video switching system, enclosures and all electrical cabling, materials, labor and equipment and services to complete a functioning video visitation system. Proposal responses should provide identified options and future capabilities.

As indicated above, the system will be implemented in multiple phases. Those phases and specific requirements are detailed below.

✓ **Securus has read, understands, and complies.**

Securus maintains end-to-end responsibility for SVV, a turnkey inmate Web-based video visitation system, at no cost to Maricopa County. Except for possible wiring needs, Securus does not require a subcontractor to install or operate SVV. We verify the completeness of all components of our system as a routine part of our installation process and continually monitor the system to ensure it operates properly and generates revenues for Maricopa County.

SVV was developed to take advantage of an open architecture that also meets ADA requirements and runs on the Internet. It also can maintain the confidentiality of attorney visitation sessions by blocking them from being recorded or monitored.

Because visitation sessions are scheduled between the SVV terminal and other party's Web-cam, third party and three-way sessions are not permitted. Further, recorded sessions and data can be downloaded to MCSO applications for investigative and statistical purposes and SVV will be capable of receiving MCSO data, such as to populate inmate accounts, inmate information, balances, etc.

The system, which will be implemented in the requested multiple phases, will consist of all required cameras, monitors, microphones/handsets, audio-video switching system, enclosures and all electrical cabling, and materials needed for ongoing operations. Securus will ensure that all labor and equipment is needed according to our preliminary implementation schedule, which can be found in Appendix A.

The system's open architecture allows the terminals to provide more than video visitation. The video visitation terminal can also serve as a kiosk to enable video arraignment and visitation

sessions between inmates and their friends or family members, attorneys, and law enforcement officers. In addition to traditional video visitation sessions, it also facilitates the following activities:

- Visitation registration and scheduling
- Inmate information application
- Sick Call application
- Securus' Secure Instant Mail (electronic mail)
- Commissary order application
- Storage of recorded visitation sessions
- Emergency video application
- Automated retrieval and playback of sessions
- Visitation reporting

Before deploying systems and upgrades—we have the most experienced staff and largest hosted architecture of all providers—Securus performs rigorous quality assurance (QA) testing to ensure minimal to no down time once it is installed. By following this discipline, you are assured that the system or upgrade performs as promised, but more important, inmates and their friends and families will be able to stay in touch and your facility will continue to earn commissions. With the largest research and development staff in the industry—more than 50 applications engineers who support current and future applications development—we develop hundreds of use cases, envisioning as many scenarios as possible, to ensure the viability of our systems. Feature updates are always provided at no cost to our customers.

Further, our R&D staff actively works to meet the emerging and evolving needs of our customers as the use of this technology matures. We seek input from our customers to learn the market-driven needs that will help craft the future of video visitation. As an important Securus customer, when Maricopa County identifies a new, high-demand need for the system, you most likely will see it in a future release.

As we look to the future of video visitation, Securus has evaluated such uses as paid secure Internet browsing, paid games, law library access, and music/MP3 sales using the Securus Video Visitation terminals.

2.2 PHASE 1 -- VIDEO VISITATION/COMMUNICATION KIOSK SYSTEM EQUIPMENT REQUIREMENTS:

Estimated implementation duration: 6 - 9 months

The Video Visitation Solution proposed for the MCSO must meet or exceed the technical requirements outlined in this Section of the RFP. The Hosted Video Visitation Solution proposed to meet these technical requirements must be provided for all MCSO facilities at no cost to MCSO including system installation, training, operation and maintenance of the system and its components.

✓ **Securus has read, understands, and complies.**

SVV meets or exceeds Maricopa County's requirements. Please refer to Appendix A for our preliminary implementation schedule.

2.2.1 VISITATION STATION LOCATIONS:

LOWER BUCKEYE JAIL (LBJ) currently has 144 video visitation stations in place; 48 total inmate visitation stations in the Tower pods; 16 total in the Dorms; 12 in the Psych unit; 6 roll-bouts in the Infirmary; 56 visitors and 6 Legal booths in the visitation lobby. LBJ is to become our central hub for visiting for all inmates in the Durango Triangle (which encompasses Durango Jail, Towers Jail, Tents Jail, Estrella Jail, and LBJ) therefore there will be a need to increase the number of visitor stations to approximately 140 visitor stations. The remaining number of stations would be inmate visitation stations which would include, but are not limited to, the following:

Towers (2 pods/tower) 11, 12, 13, 14, 21, 22, 23, 24, 31, 32, 33, 34:

(3) Legal (rooms provided)

(1) Medical/Legal consultation (room provided)

(2) Inmate visiting stations

Dorms 1, 2, 3, 4:

(1) Medical/Legal consultation

(2) Inmate visiting stations

Psych P1, P2, P3, P4, P5, P6:

(1) Inmate visiting stations (All purpose)

Infirmary:

(12) Roll-bouts

4TH AVENUE JAIL currently has 115 video visitation stations in place; 56 total inmate visitation stations in the Tower pods; 14 roll-bouts in the Special Management Unit (SMU); 38 visitors and 7 Legal booths in the visitation lobby. 4th Ave is to become our central hub for visiting for all inmates in the Downtown Area therefore there will be a need to increase the number of visitor stations to approximately 50 visitor stations. The remaining number of stations would be inmate visitation stations which would include, but are not limited to, the following:

Houses (2 pods/house) 2A, 2B, 2C, 2D, 2E, 2F, 3A, 3B, 3C, 3D, 3E, 3F:

(3) Legal (rooms provided)

(1) Medical/Legal consultation (room provided)

(2) Inmate visiting stations

Houses (2 pods/house) 4A and 4F:

- (3) Legal (rooms provided)
- (1) Medical/Legal consultation (room provided)
- (2) Inmate visiting stations

Houses (4 pods/house) 4B and 4E: (16) Roll-bouts

SMU 1-4 runs:

- (8) Roll-bouts

TENTS JAIL currently has 61 video stations in place; 36 total inmate visitation stations in the Dorm area; 25 total visitor booths. Since we are going to have the central hub at LBJ there is no need to have visitor side locations, but inmate booths' are to remain a current numbers:

N Dorm: (26) Inmate visiting stations

- (3) Legal/Medical (sound proofing booths must be provided)

O Dorm: (10) Inmate visiting stations

- (4) Legal/Medical (sound proofing booths must be provided)

DURANGO JAIL currently has no video visitation system in place. Once the new system is installed all visitors will utilize the LBJ Visitor Center or use the web-based application portion to obtain their visits. The remaining number of stations would be inmate visitation stations which would include, but are not limited to, the following:

Houses (4 pods/house): D1, D2, D3, D4, D5, D6, D7:

- (5) Inmate visiting stations

- (1) Legal (sound proofing booths must be provided)

Houses D8 and D9 (Dorms):

- (6) Inmate visiting stations

- (3) Legal/Medical (sound proofing booths must be provided)

TOWERS JAIL currently has no video visitation system in place. Once the new system is installed all visitors will utilize the LBJ Visitor Center or use the web based application portion to obtain their visits. The remaining number of stations would be inmate visitation stations which would include, but are not limited to, the following:

Towers (4 pods/tower) T1, T2, T3, T4, T5, and T6: (3) Inmate visiting stations

- (1) Legal/Medical (sound proofing booths must be provided)

ESTRELLA JAIL currently has no video visitation system in place. Once the new system is installed all visitors will utilize the LBJ Visitor Center or use the web based application portion to obtain their visits. The remaining number of stations would be inmate visitation stations which would include, but are not limited to, the following:

Houses A, C, D (4 pods/house):

(2) Inmate visiting stations

(1) Legal/Medical (sound proofing booths must be provided)

House B (3 pods of CC):

(6) Roll-bouts

House B (1 pod normal):

(2) Inmate visiting stations

(1) Legal/Medical (sound proofing booths must be provided)

Dorms E, F, G, H, I, J, K, L:

(3) Inmate visiting stations

(1) Legal/Medical (sound proofing booths must be provided)

Dorm M (3pods):

(1) Inmate visiting stations

The minimum acceptable replacement system shall have the minimum stations indicated above and be expandable at no charge. If the initial system has usage of 50% or more of any one station for more than one month an additional station shall be installed. The expansion shall occur within seven days.

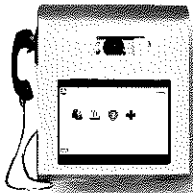
✓ **Securus has read, understands, and complies.**

2.2.2 EQUIPMENT SPECIFICATIONS:

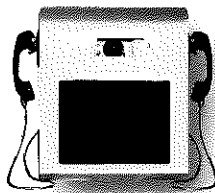
Kiosk Video machines furnished under this contract shall be a hardened steel enclosure to include a touchscreen. The Kiosk Video station must be new or in like-new condition and appearance, in good working condition, and fully operable when installed and during the contract period. The equipment must be approved by MCSO before installation.

✓ **Securus has read, understands, and complies.**

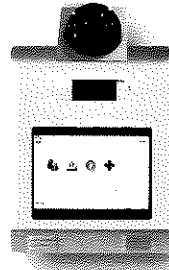
The SVV terminal is constructed as a self-contained, hardened steel case that is wall mounted and equipped with a built-in shatterproof touch screen, a high-resolution video camera with integrated lighting, and a handset for audio communication. However, the tamper-resistant terminals can be mounted in other ways if needed, as shown in the following illustration.



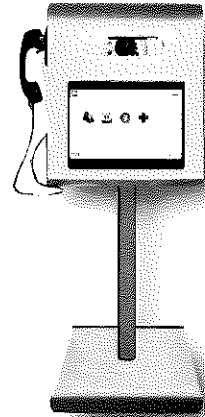
One handset, usually installed inside the housing locations with the inmates.



Two handsets, primarily for visitors.



Hands-free for medical / court / family visits (with PTZ 360° camera).



Units can be mobile or mounted on a pedestal or wall.

The steel braided corrections-grade handset can withstand 1,000 pounds of pressure. Surge protection is implemented on each unit with the ability to maintain clean power in the event of a brown-out, where the voltage drops to 6V. The stations come with a custom mounting bracket that ensures a secure, vandalism-proof installation that also prevents hiding of any contraband within or behind the terminal. On the rear of the station the only cables to connect are power and networking: a 3-prong 120-volt (standard PC power cable) and a CAT6 networking cable. The stations do not require additional cabinetry. All equipment will be approved by MCSO before installation.

- 2.2.3 Detention grade hardened steel wall mounted enclosure with rounded top and corners.

✓ **Securus has read, understands, and complies.**

As illustrated above, Securus SVV terminals meet this requirement.

- 2.2.4 A shatterproof LCD touchscreen monitor with a minimum of 15" and no larger than 17".

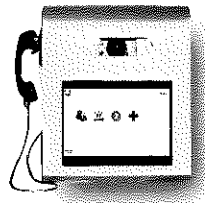
✓ **Securus has read, understands, and complies.**

SVV terminals feature shatterproof 15-inch touch screens.

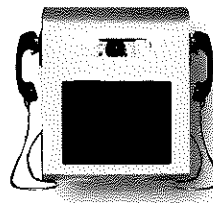
- 2.2.5 One detention grade audio handset per inmate terminal, and two detention grade audio handsets per visitor terminal, and have portable terminals with handset and speaker option.

✓ **Securus has read, understands, and complies.**

Handsets on SVV terminals are detention grade—one on inmate terminals and two on visitor terminals, as shown in the illustration below.



One handset, usually installed inside the housing locations with the inmates.

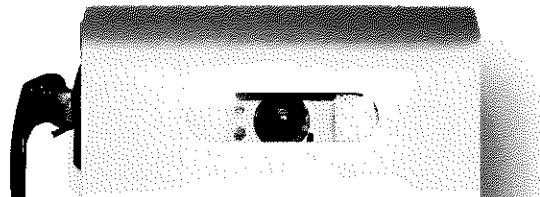


Two handsets, primarily for visitors.

- 2.2.6 The terminal will have a built-in camera with built-in LED lighting that automatically activates during video visitation sessions and automatically ends when the video visitation session completes.

✓ **Securus has read, understands, and complies.**

SVV terminals have built-in cameras and unique LED lighting to illuminate inmates and those in the visitor center so they can better be seen and also assists in the monitoring and investigative functions. The following picture highlights the camera and LED light area of the terminal.



- 2.2.7 The enclosure shall not have any openings exposed to the user. This includes all wiring and ventilation holes.

✓ **Securus has read, understands, and complies.**

SVV terminals do not have any openings exposed to users, including those for wiring and ventilation.

2.2.8 The enclosure shall not have any external hinges.

✓ **Securus has read, understands, and complies.**

SVV terminals do not have any external hinges.

2.2.9 The terminal must prevent spills from entering the enclosure.

✓ **Securus has read, understands, and complies.**

SVV terminals are sealed so that no spills can enter the enclosure.

2.2.10 The terminal must have on-screen signature capabilities to capture an inmate's signature without the use of a "light pen" or other external attachment.

✓ **Securus has read, understands, and complies.**

Because SVV terminals are hardened touch screens, they are capable of accepting signatures "written" without having to use a "light pen" or external attachment that could be used as a makeshift weapon within the facility. Currently we use PINs or other identifiers to determine which inmates are using the system.

2.2.11 The terminal must be assembled from non-proprietary, off-the-shelf computer components.

✓ **Securus has read, understands, and complies.**

Terminals are made of nonproprietary commercial off-the-shelf computer components, units can be returned to Securus for service.

2.2.12 The terminal shall be powered by 110VAC.

✓ **Securus has read, understands, and complies.**

SVV is available for immediate installation and use by Maricopa County and requires either 110 volt AC or low-voltage direct current.

- 2.2.13 The terminal must have heat syncs and heat vents, located in the back of the terminal, in order to allow for proper cooling.

✓ **Securus has read, understands, and complies.**

SVV terminals have fans as well as heat syncs and heat vents in the back for proper cooling. The venting is designed to protect against spills.

- 2.2.14 The enclosure shall not have a physical on/off switch; it must be able to be remotely shut off by a staff member using a switch located in a secure area.

✓ **Securus has read, understands, and complies.**

SVV terminals do not have a physical on/off switch on their exterior. Rather a proprietary magnet is used to activate and de-activate the terminals, preventing inmates from powering them on or off. The software that operates the SVV terminals can be disabled remotely, effectively shutting the terminal off.

- 2.2.15 The system must have a LCD "wallboard" viewing officer's station at each facility.

✓ **Securus has read, understands, and complies.**

Authorized MARICOPA users will be able to initiate, control, record, retrieve and monitor video visitation sessions. One of the primary advantages of implementing SVV is the ability to live monitor and record video visitation sessions. This capability creates new investigative opportunities and also reduces violence within jail walls. In addition, the SVV interface enables jail staff to flag visits for later investigative review and lock recordings from being purged after the standard retention window expires.

SVV sessions can be monitored live by facility administrators by clicking on the "Appointments" icon and then selecting "View." Multiple live sessions can be viewed simultaneously. There are no software-imposed limitations regarding the number of sessions that can be viewed at the same time. Simultaneous sessions will be limited by available bandwidth.

- 2.2.16 The "wallboard" station must be a minimum of 47" viewing platform with an array of different configurations for viewing multiple visits simultaneously with the ability from the viewing station to end visits remotely due to improper conduct.

✓ **Securus has read, understands, and complies.**

Authorized users can monitor several video sessions simultaneously depending on the capacity and capabilities of the user's personal computer and monitor. This capability is on Securus'

development road map for SVV. Authorized personnel who are monitoring sessions have the ability to end sessions, such as due to improper conduct by any party during a session.

2.3 WEB-BASED VIDEO VISITATION/COMMUNICATION KIOSK SYSTEM HARDWARE REQUIREMENTS:

- 2.3.1 Digital Recording - The system must include digital recordings of video conversations, in real-time and with historical and playback capability. These recordings can be selectively turned on or off through programming by the vendor, dependent on the type of call and other pertinent legal requests. Describe the process.

✓ **Securus has read, understands, and complies.**

One of the primary advantages of implementing video visitation is the ability to live monitor and record video visitation sessions. This capability creates new investigative opportunities and also reduces violence within jail walls. In addition, the SVV interface enables jail staff to flag visits for later investigative review and lock recordings from being purged after the standard retention window expires.

Securus understands that for video visitation to work effectively with the unique demands of the corrections environment, it must be user-friendly and intuitive for Maricopa County staff. The SVV Dashboard, depicted in the following graphic, was developed to enable users to quickly and easily manage all of the facility tasks associated with video visitation, such as:

- User account approval and management
- Schedule management
- Reporting
- Live monitoring
- Playback of recorded sessions
- Information Portal for efficiency-driving applications such as Sick Call, Emergency Call, and commissary ordering

Securus Video Visitation Dashboard

Securus Video Visitation

Welcome, [User Name] | Online | 11:15 AM | CPT | Logout

Appointments

Appointments | New appointment | New appointment for others | New public appointment | Reports

Emergency call

Communications

Chat | Messages

Administration

Home > Appointments > Reports

Users | Groups | Logs | Parameters

Session Viewer

Session Viewer | Parameters

Commissary

Products | Product Fair

Medical

Symptoms | Calls

Report list

ID	Type	User list	Date	Start time	Duration	Status	Actions
576	Regular	Walter Bond (197) - Securus OA - Institution Securus CA - 0-1	2012-05-06	00:00:00	15	Failed	[Icon]
492	Public	Walter Bond (197) - Securus OA - Institution Securus CA - 0-1	2012-05-06	00:00:00	15	Failed	[Icon]
576	Public	Walter Bond (197) - Securus OA - Institution Securus CA - 0-1	2012-05-06	00:00:00	15	Failed	[Icon]
576	Public	Walter Bond (197) - Securus OA - Institution Securus CA - 0-1	2012-05-06	00:00:00	15	Failed	[Icon]

Appointment list

ID	Type	User list	Date	Start time	End	Duration	Status	Actions
576	Regular	Walter Bond (197) - Securus OA - Institution Securus CA - 0-1	2012-05-06	00:00:00	00:15:00	15	Failed	[Icon]
576	Regular	Walter Bond (197) - Securus OA - Institution Securus CA - 0-1	2012-05-06	00:00:00	00:15:00	15	Failed	[Icon]

Session Viewer

Session	Appointment	User list	Date	Start	End	Duration	Actions
576	576	Walter Bond (197) - Securus OA - Institution Securus CA - 0-1	2012-05-06	00:00:00	00:15:00	15	[Icon] [Icon] [Icon]
576	576	Walter Bond (197) - Securus OA - Institution Securus CA - 0-1	2012-05-06	00:00:00	00:15:00	15	[Icon] [Icon] [Icon]

25 total results

Visitation sessions not blocked from recording are automatically recorded and can be played back at any time.

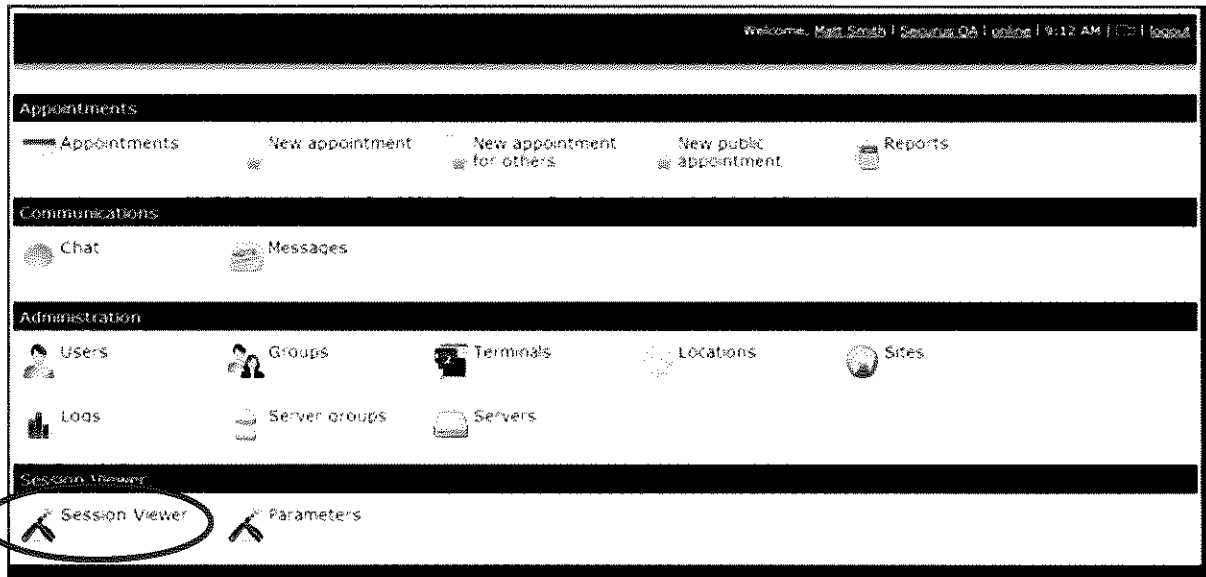
Live Monitoring:

SVV sessions can be live monitored by facility administrators by clicking on the "Appointments" icon and then selecting "View." Multiple live sessions can be viewed simultaneously. There are no software-imposed limitations regarding the number of sessions that can be viewed at the same time. Simultaneous sessions are limited only by the available bandwidth.

Viewing a session is as simple as a mouse-click on the Session Viewer, as the following screen capture shows.




Selecting Session Viewer in SVV

Proprietary and Confidential



Download Recordings

The ability to live monitor, record, and retain video visitation sessions is extremely important to Maricopa County and Securus. Although Securus stores all recorded videos for the agreed upon duration (standard 30 days), we understand that there are times when visits must be retained for an even greater amount of time. To do this, Securus enables authorized facility administrative users to download recorded video visitation sessions.

To view a list of recorded visits, authorized users will simply log in to the system from a computer with internet access and select the updated "Session Viewer" icon ( Session Viewer). From the Session Viewer, facility personnel can use existing functionality to convert the file to a viewable format by selecting the "Request Conversion" icon () or download the file by selecting the new "Download" icon (). These functions are shown in the following screen capture.

Downloading SVV Recordings

Proprietary and Confidential

The screenshot shows the 'Video Visitation' interface. At the top, it says 'Welcome, Matt Smith | Securus, GA | 2/11/13 PM CT | online | [?] | Logout'. Below the navigation bar, there are tabs for 'Session Viewer' and 'Parameters'. The 'Session Viewer' tab is active, displaying a table with the following data:

Session	Appointment	User list	Date	Start	End	Duration	Actions
1277	2585	James Bond Jim Yang	2013-01-17	04:00:15 AM CT	04:05:15 AM CT	05:00:00	[Play] [Lock] [X] [Download]
1277	2584	James Bond Jim	2013-01-16	10:10:30 AM CT	10:40:15 AM CT	00:29:45	[Play] [Lock] [X] [Download]
1275	2583	Jim Jim Jim	2013-01-17	04:00:15 AM CT	04:10:15 AM CT	00:01:00	[Play] [Lock] [X] [Download]

At the bottom of the table, it says '3 results (page 1 of 1)'. An 'Actions' menu is shown on the right, with a download icon (a document with a downward arrow) highlighted by a red arrow.

If the download icon is selected and the visitation session has not been previously converted, the "Download" and "Request Conversion" icons will change to clocks (🕒) and a green status bar will appear. This improved feedback mechanism visually enhances the usability of SVV and informs users of system operations as they are happening.

Video Conversion Confirmation

Proprietary and Confidential

The screenshot shows the 'Session Viewer' interface with a single session displayed:

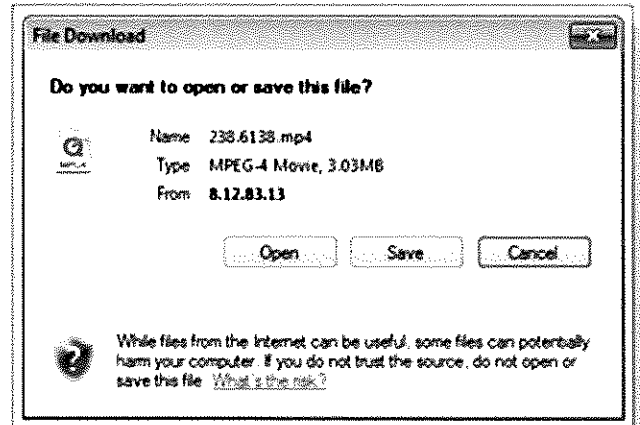
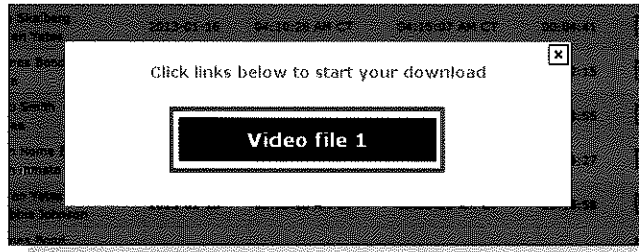
Session	Appointment	User list	Date	Start	End	Duration	Actions
6138	8933	James Bond Jose Castro	2013-01-16	04:30:40 AM CT	04:32:05 AM CT	00:01:25	[Clock] [Lock] [X] [Clock]

Below the table, a green status bar displays the message: '*** Processing request, please wait until the icon gets updated'.

Once the conversion process is complete, simply click on the "Download" icon again, select "Video file 1" from the pop-up window, and choose to either save or open the file.

Accessing Downloaded Video File

Proprietary and Confidential



Visits can also be downloaded while viewing a recorded session by clicking on "Video file 1."

Viewing Downloaded Video File

Proprietary and Confidential



Recorded visitation sessions are downloaded in MPEG-4 format. Most computers come equipped with media players that are compatible with this format; however, there are also many free downloadable media players available from Adobe, Real Player, videolan.org and other developers.

Recording of video sessions will be suspended for privileged visitation sessions, such as attorney visits. Attorneys must register in SVV in a custom user group, which will be used as the key to whether a visitation session is recorded or not.

Registration Process

The following outlines the registration process in which users set up SVV accounts.

Friends, family members, attorneys and other remote users create Securus Video Visitation accounts by going to VideoVisitation.securustech.net. The user's computer will automatically be scanned to verify whether the appropriate software is installed and ensure their web camera will enable a quality visit and prevent future visitation issues for the user. Software includes:

- JavaScript
- Adobe Flash Player
- Microsoft Windows (Mac compatibility coming soon)
- Java Runtime

If any of the tests fail, a link will be provided to download any needed applications. Consumers can also choose to manually test their webcam by clicking on: "Test your web camera."

Users will choose to either create their account as a friend and family member or as an attorney. Attorney accounts will require additional verification, such as a Bar ID.

Welcome to Securus Video Visitation

Before signing up please be sure you have

- a Webcam
- a valid ID with picture or attorney ID
- a credit card (Visa or Mastercard) or a debit card

Requirements	Status
JavaScript	✓ Installed and available
Adobe Flash Player	✓ Installed and available
Microsoft Windows	✓ Installed and available
Java Runtime	✓ Installed and available
Web Camera	Test your web camera

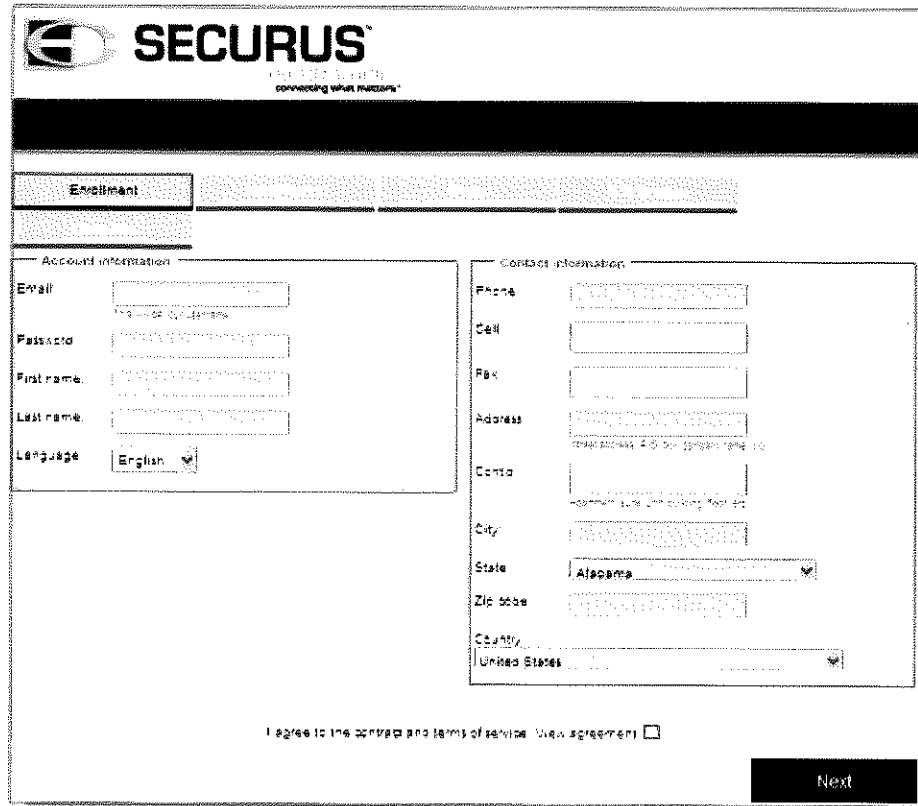
↓↓↓ REGISTER HERE ↓↓↓

For friends and family members

For attorneys

Step 1: Enrollment

Users will need to complete the enrollment form, which includes email address, first name, last name, telephone number, address, and password. Fields highlighted in gold are required.



The image shows a web-based enrollment form for Securus. The form is titled "SECURUS" with the tagline "connecting what matters". Below the title is a navigation bar with "Enrollment" highlighted. The form is divided into two main sections: "Account information" and "Contact information".

Account information:

- Email:
- Password:
- First name:
- Last name:
- Language:

Contact information:

- Phone:
- Cell:
- Fax:
- Address:
- City:
- State:
- Zip code:
- Country:

At the bottom of the form, there is a checkbox labeled "I agree to the contract and terms of service. View agreement" and a "Next" button.

Step 2: Identification

Users will be required to provide a picture of approved identification such as a driver's license.

The screenshot shows the 'Identification' step of the Securus system. At the top, a header bar contains the word 'Identification'. Below it, a message states: 'We require a copy of an identification card before we can allow access to the Securus Video Visitation system.' The interface is divided into four steps:

- Step 1: click 'Allow'**: Shows a small window with a 'Yes' button.
- Step 2: place your license in front of the camera**: Shows a camera view of a person's license.
- Step 3: click 'Capture'**: Shows a 'Capture' button.
- Step 4: click 'Save'**: Shows a 'Save Image' button.

Below the steps, there are two large images of a Securus identification card for Matthew Smith. At the bottom, there are 'Previous' and 'Next' buttons.

Step 3: Photo

Users will be required to take a self portrait.

The screenshot displays a web-based interface for uploading a photo. At the top, there is a 'Photo' button. Below it, a message states: 'We require a copy of a photo of yourself before we can allow access to the Securus Video Visitation System'. The interface is divided into four steps:

- Step 1: Click Allow**: A small thumbnail of a photo.
- Step 2: Place yourself in the middle of the camera**: A larger camera view showing a man's face.
- Step 3: Click Capture**: A button labeled 'Capture'.
- Step 4: Click Save**: A button labeled 'Save Image'.

Below the steps, there are two side-by-side camera views showing the same man's face. At the bottom, there are buttons for 'Previous', 'Capture', and 'Save Image'.

Step 4: Confirmation

Users will be given the opportunity to review all of their information and provide final confirmation before the account is created.

Confirmation

Account Information

Email: matthewsmith@securus-tech.net
 First name: Matthew
 Last name: Smith

Contact Information

Phone: 972-277-0689
 Cell:
 Fax:
 Address 1: 14851 Dallas Parkway
 Address 2:
 City: Dallas
 Zipcode: 75254
 State: Texas
 Country: United States

Photos

Billing Information

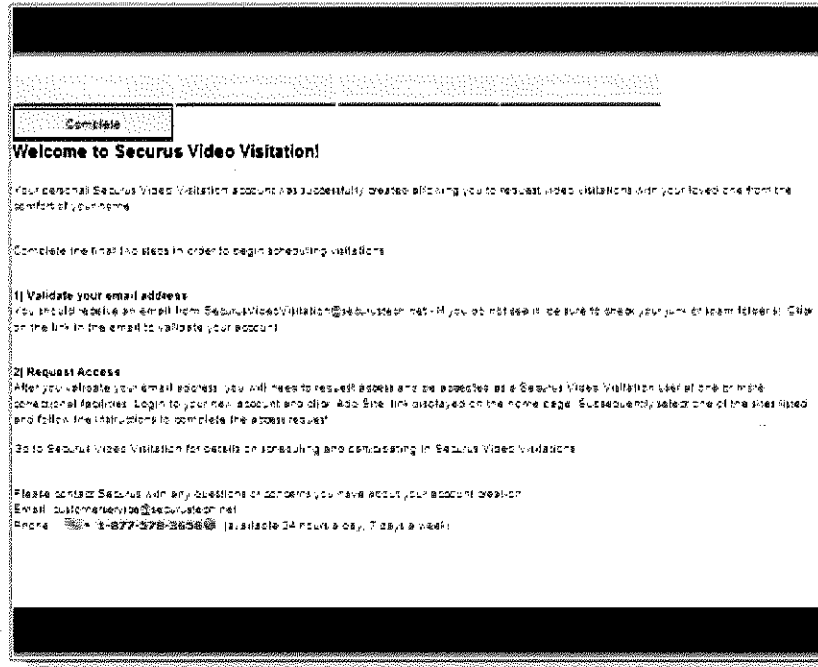
Name: Matthew Smith
 Email: matthewsmith@securus-tech.net
 Phone: 972-277-0689
 Address 1: 14851 Dallas Parkway
 Address 2:
 City: Dallas
 Zipcode: 75254
 State: TX
 Country: United States

Use a different billing address

Previous **Next**

**Users are given 10 minutes to complete each of the four (4) account creation steps before the software automatically times out.*

Once all steps are completed, users will be instructed to validate their account by clicking on a link in the introduction email and to request access to a specific Securus Video Visitation site.



After completing the process, facility personal must approve and authorize the user's registration before visitation sessions can be scheduled. This process allows Maricopa County to verify a visitor's eligibility to visit with an inmate.

- 2.3.2 Recording Backup - The system shall be equipped with appropriate backup, to reduce interruption of service or data loss. Describe the process.

✓ **Securus has read, understands, and complies.**

The video visitation application and data reside on a server that is hosted on Securus' network. This server manages all the interactions between the video visitation terminals and clients and provides secure storage of all data.

All servers located in the Securus data centers are regularly backed up, and geographically redundant, to ensure the highest quality of service and reduce the potential for service interruption or data loss.

- 2.3.2.1 Legal IP Number Database - The system shall have the capability to allow entries of the name associated with the IP number, law firm, probation, or court and date the IP number was added.

✓ **Securus has read, understands, and complies.**

Rather than rely on IP addresses, SVV streamlines this process and reduces database needs because it requires attorneys to register using their Bar ID, which is described in the registration process above in our response to 2.3.1. Through this process and final verification by facility personnel, attorney visits are kept confidential though a record of the visitation session is still retained.

- 2.3.3 Non-Record Legal Video - Legal Video Visits shall not be recorded. Describe how the system ensures that a video to a legal visit is not recorded.

✓ **Securus has read, understands, and complies.**

The system Securus proposes is an integrated IP-based, real-time, corrections-based communication system. SVV is a combination of state-of-the-art video conferencing technology, browser-based network control and scheduling, and enterprise-level computing and storage with the most sophisticated digital recording and monitoring on the market today. Each unit delivers fully integrated, corrections-based technology solution in a single system deployment.

Securus follows the same privacy protocol as all states and government agencies, which require that all privileged visits, such as attorney-inmate sessions, not be recorded.

- 2.3.4 Reproducing Media - Writeable DVD or Blu-ray are the preferred reproducing media to include encrypted password capability. Describe the process used by your system.

✓ **Securus has read, understands, and complies.**

Recorded sessions can be downloaded and copied to any recording media or emailed.

- 2.3.5 Uninterrupted Power Supply (UPS) - The system shall include a UPS backup for use in the event of a commercial power interruption. Describe your system UPS backup.

✓ **Securus has read, understands, and complies.**

Because Securus hosts SVV from our state-of-the-art data center, the central system is protected on our premises. Securus also provides UPS for the routers it installs at the Maricopa County Jail to ensure they always have ample protection.

- 2.3.6 Time Synchronized System to a Master Clock - The entire system shall be time synchronized including automatic daylight saving adjustment and Arizona time, to the MCSO time sync server through a Uniform Resource Locator (URL) or IP address.

✓ **Securus has read, understands, and complies.**

Securus synchronizes SVV with all time zones to ensure the integrity of time and date data across the system. This synchronization includes adjusting for changes in daylight savings time and Arizona time.

2.3.7 Firewall - Describe your Firewall protection system.

✓ **Securus has read, understands, and complies.**

Securus will install and maintain firewalls both on site and at our centralized data center in Dallas, TX.

On site, data is both encrypted and authenticated via software algorithms. This occurs at both the inmate video terminal, at on-site friends and family terminals, and at the PC of a home user (during remote visitation sessions).

At our corporate data center, for video traffic from our facilities we utilize a redundant pair of Cisco 5540 Adaptive Security Appliances for the Firewall. For the remote web services, we use an independent, redundant pair of Cisco 5540 Adaptive Security Appliances for the Firewall.

2.3.8 Archival of Records and Recording

2.3.8.1 Contractor shall provide a storage facility for all data.

✓ **Securus has read, understands, and complies.**

SVV sessions are stored in Securus' data center.

2.3.8.2 Records - The records shall be stored and available online for a period of three (3) year, or 1095 days.

✓ **Securus has read, understands, and complies.**

Securus will store records for three years and have them available online as Maricopa County requires.

2.3.8.3 Recordings - The recordings shall be stored and available online, for a minimum period 3 months, or 90 days.

✓ **Securus has read, understands, and complies.**

We can store recordings for 90 days as Maricopa County requires.

2.3.8.4 MCSO shall retain all rights and ownership for data of records and recordings.

✓ **Securus has read, understands, and complies.**

MCSO will retain all rights and ownership for data of records and recordings.

2.4 VIDEO VISITATION SYSTEM SOFTWARE REQUIREMENTS:

2.4.1 The video visitation scheduling, user management, and policy management, must be web-based and allow for MCSO to administer visitation sessions and visitation operations based on MCSO policies

✓ **Securus has read, understands, and complies.**

SVV makes the complex tasks of scheduling sessions and managing user accounts easy and secure for the facility, friends and family members, and inmates. The following highlights many of the features and functions inherent in SVV.

User Account Set-up and Scheduling for Friends and Family Members

- Web-based and accessible from any standard Web browser
- Simple user interface, enabling account set-up and scheduling to be completed in minutes
- Automatically support multiple facilities in multiple locations with multiple housing units, making it easy to "find" the desired inmate
- Automatically displays only the visitation times and dates that are available
- Automatically sends an email confirmation when a visit is scheduled, modified, or cancelled
- Allows users to easily change their personal information (password, address, phone number, etc.)

Secure, At-Home Visitation Scheduling

Home > Appointments > New appointment

Appointments New appointment

New appointment

Users point and click New Appointment, search for their inmate, and select a desired date and time for a visitation session.

Date: 2012-04-02

Duration: 1:00:00

Inmate: 007 James Bond

Time: 12:45 P.M.

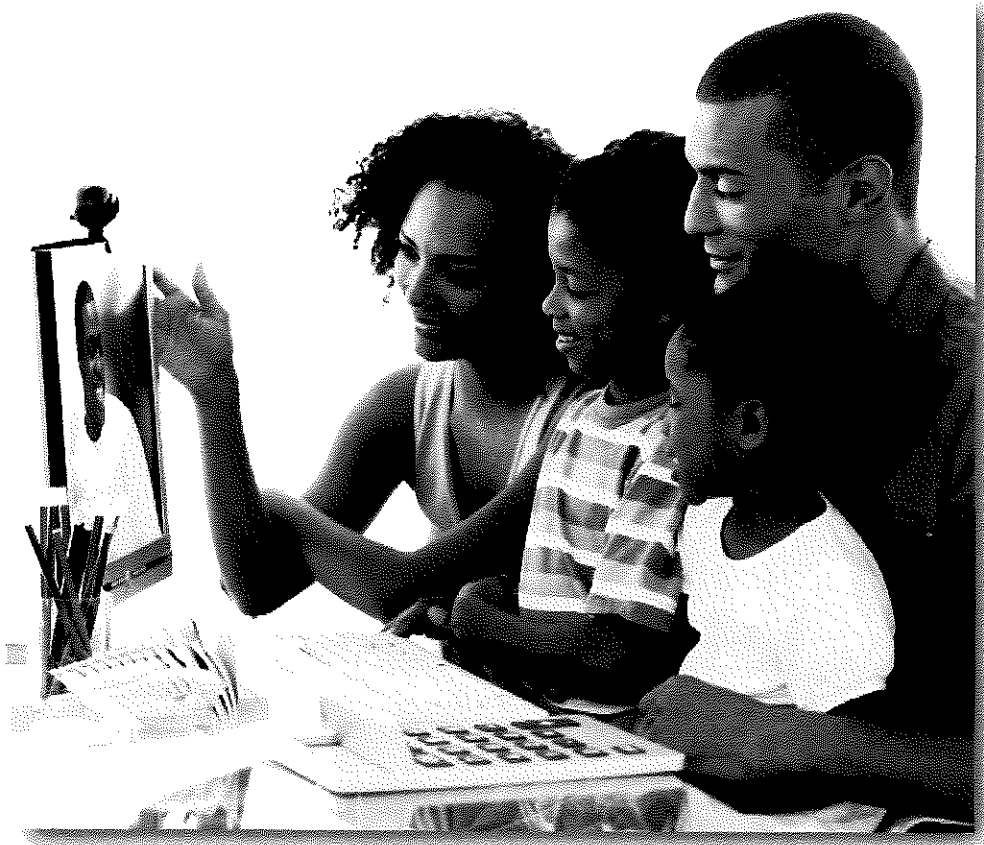
Go to previous step Save Reset

User Account Control and Scheduling Features for the Facility

- Secure, Web-based access anytime/anywhere – providing different levels of authority and requiring unique user names and passwords
- Point and click to view thorough user information including photo ID and easily approve or reject a user account
- View, manage, report, and modify scheduled visits from the SVV dashboard
- Review historical staff usage through system user logs

Scheduling Features for Inmates

- Terminals with simple touch screens and user-friendly, basic icons - providing inmate access in English, Spanish, and any other language requested by Maricopa County
- Large letters and numbers that clearly display pending visits
- Built in lighting to enhance screen images
- On-screen timer to show remaining time throughout the entire visitation session



2.4.1.1 Legal Visits (Private Attorneys) - Legal Visits are considered right to counsel confidential. These videos are not recorded or monitored and may be charged for Web usage.

✓ **Securus has read, understands, and complies.**

While attorney calls are private and not recorded, they still are logged and charged so that Maricopa County can earn commission payments on them and track the activity. Records of all visits that have occurred are stored even though the visit is not recorded. This valuable information shows that attorneys have had access to their clients. Records are stored for three years.

2.4.1.2 Legal Visits (County Public Defenders/Prosecutors)-Legal Visits are considered right to counsel of confidential. These videos are not recorded or monitored and will not be charged Web usage.

✓ **Securus has read, understands, and complies.**

While attorney calls are private and not recorded, they still are logged and charged and Maricopa County can earn commission payments on them. There is a record of all visits that have occurred. This valuable information shows that attorneys have had access to their clients. Records are stored for three years.

- 2.4.1.3 Free County Agency Visits (i.e. Adult Probation, Sheriff's Deputies, and Officers of the Court) - These videos are not considered right to counsel confidential. The Video is recorded and monitored and is free from Web usage.

✓ **Securus has read, understands, and complies.**

Securus records all visitation sessions that are not private and privileged. Securus will work with Maricopa County to establish custom user groups that identify sessions for which there will be no charge to users.

2.5 SYSTEM FEATURE REQUIREMENTS:

- 2.5.1 Inmate Personal Identifier (PIN) - The system shall provide unique Personal Identification number to each inmate and user. The system shall interface with MCSO's Jail Management System (JMS). Inmates shall establish a PIN number upon first use of kiosk system.

✓ **Securus has read, understands, and complies.**

Securus has solid, proven experience with integration and currently integrates with more than 110 vendors worldwide and over 60 independent facility-owned systems and shared databases.

Securus has its own dedicated Integration Department that works exclusively on integrating the various systems and products in the corrections environment. Having this dedicated Integration Department allows Securus to deliver fast and flexible solutions for our customers. Securus' technology is flexible and does not mandate rigid specifications when working with facility-owned systems, JMS, OMS, commissary, vendors, etc. Securus will fully cooperate with your facilities and vendors to automate the systems.

The most common technologies Securus uses to integrate with your systems include: SOAP Web Services, HTTP, FTP push or pull of files in any textual format, JSON, XML-RPC, and TCP Sockets. All of these methods are performed over a secure connection.

Securus is able to transform your data format for insertion into our platform, negating the need for costly code modifications to your system. Securus integration engineers will consult with your facilities' IT department or system provider to determine the best integration strategy for your specific application.

Securus Integration Process

The dedicated Securus Integration team designs, develops, tests, and implements all custom integrations with corrections industry and banking systems. Our mission is to deliver fast and flexible solutions for our customers. This process is incorporated into the overall Project Plan, included as Appendix A, for the installation of the Securus SCP inmate telephone system. Major milestones include:

- Collect Preliminary Needs/Requirements
- Contract Signed
- Finalized Requirements document
- Approved Scope Statement
- Finalize Design Document
- Schedule Customer Implementation
- Develop Custom Integration Solution
- Test Custom Integration Solution
- Implement Custom Integration Solution
- Customer Approval and Sign-off

2.5.2 Multi-lingual inmate interface (English and Spanish at a minimum).

✓ **Securus has read, understands, and complies.**

SVV's terminals have simple touch screens and user friendly, basic icons - providing inmate access in English, Spanish, and any other language requested by Maricopa County

2.5.3 A single system must be able to support multiple facilities in multiple locations with multiple housing units.

✓ **Securus has read, understands, and complies.**

Because SVV is Web based, it easily supports multiple facilities.

2.5.4 Web-based visitation scheduling for authorized users (MCSO Services staff, attorneys, the public) utilizing any standard web browser.

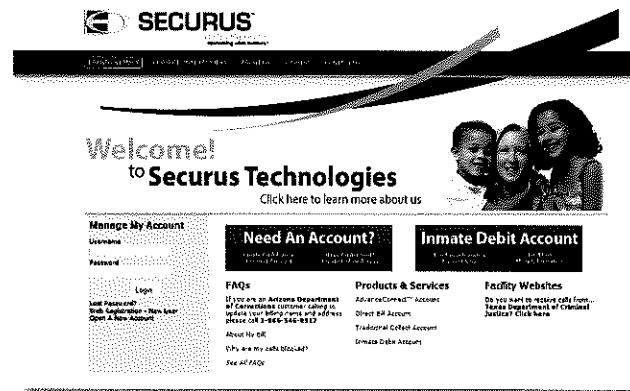
✓ **Securus has read, understands, and complies.**

Inmates' friends and family members access a simple Web site via the Internet, designed with the look and feel of other Securus systems. The inmate's friend or family member schedules and pays for a video-visitation session by going to www.securustech.net Web site.

Using the video visitation Web site, they can select the facility and inmate they wish to participate in the video visitation session. The scheduling application automatically schedules visits according to the inmate's dormitory, which terminals are available at that location, and available session times for video visitations to be held. Fees are assessed and collected at the time the visit is scheduled via credit or debit card.

SVV receives inmate information, including housing location, from the JMS. Our system then dynamically identifies whether the inmate is located in an area with a video visitation terminal, whether a terminal is available based on date/time of the requested visit, and automatically displays only available times to the person scheduling the session.

SVV allows user fees to be assessed for remote or at-home visitation sessions and collected by the system. As friends and family or members of the public elect to conduct remote visitation sessions, they pay for the session on a per-session charge.



- 2.5.5 Inmate terminal must display pending visits and scheduled medical appointments.

✓ **Securus has read, understands, and complies.**

By touching on the appointments icon the SVV terminal screen, inmates can see that day's pending visitation sessions. However, the system shows that only a session is scheduled and does not define the kind of session, such as a medical appointment, providing privacy for inmates and conformance with HIPAA requirements.

- 2.5.6 Web-based scheduling system must allow users to easily and simply schedule a visitation session.

✓ **Securus has read, understands, and complies.**

Inmates' friends or family member schedule and pay for a video-visitation session by going to www.securustech.net web site and following the easy-to-understand prompts.

- 2.5.7 Web-based scheduling system must require visitors to provide valid photo ID in accordance with MCSO Policy DK-3, Inmate Visitation before signing up for a visitation session.

✓ **Securus has read, understands, and complies.**

Friends and family members are required to provide proof of identity when registering for SVV. Failure to do so nullifies their enrollment and prevents them from being able to schedule visitation sessions. Friends and family members' identities can be easily verified by authorized Maricopa County users.

- 2.5.8 Web-based scheduling system must only display timeslots that are available for each individual inmate in conjunction with JMS and other scheduled Inmate functions included but not limited to future court dates, medical appointments, and programs.

✓ **Securus has read, understands, and complies.**

SVV displays only available time slots to friends and family members to avoid double-booking appointments. Inmates can easily see appointments scheduled for that day by pressing the Appointments icon on an SVV terminal. To track inmates, SVV interfaces with the JMS and takes data feeds approximately every 15 minutes. If an inmate is moved to court or the infirmary, for example, any sessions scheduled for that inmate during that time period will be automatically cancelled and notification sent to the individual who scheduled the session.

- 2.5.9 Web-based scheduling system must conduct all conflict checking and only display times that are available.

✓ **Securus has read, understands, and complies.**

SVV displays only times that are available.

- 2.5.10 Web-based scheduling system must allow users to easily change their personal information (password, address, phone number, etc.).

✓ **Securus has read, understands, and complies.**

Users can easily manage their accounts through SVV's Web portal.

User Account Set-up and Scheduling Features for Friends and Family Members

- Web-based and accessible from any standard web browser
- Simple user interface, enabling account setup and scheduling to be completed in minutes
- Automatically support multiple facilities in multiple locations with multiple housing units, making it easy to "find" the desired inmate
- Automatically display only the visitation times and dates that are available

- Automatically send an email confirmation when a visit is scheduled, modified, or cancelled
- Allow users to easily change their personal information (password, address, phone number, etc.)

Secure, At-Home Visitation Scheduling

Home > Appointments > New appointment

Appointments New appointment

New appointment

Users point and click New Appointment, search for their inmate, and select a desired date and time for a visitation session.

Date: 2012-04-02

Duration:

Inmate: 007 James Bond

Time: 12:45 PM

Go to previous step | Save | Reset

User Account Control and Scheduling Features for the Facility

- Secure, web-based access anytime/anywhere – providing different levels of authority and requiring unique usernames and passwords
- Point and click to view thorough user information including photo ID and easily approve or reject user account
- View, manage, report, and modify scheduled visits from the Securus Video Visitation dashboard
- Review historical staff usage through system user logs

2.5.11 Web-based scheduling system must send an email to the visitor when a visit is scheduled, modified, or cancelled.

✓ **Securus has read, understands, and complies.**

During account set-up and scheduling, SVV will automatically send an email confirmation when a visit is scheduled, modified, or cancelled.

- 2.5.12 If a scheduled visit is cancelled, the timeslot should become available for scheduling.

✓ **Securus has read, understands, and complies.**

If a timeslot becomes available for any reason it will automatically be available to be scheduled by others.

- 2.5.13 Web-based scheduling system must assign a unique visitation identification number for every visit for reporting and tracking.

✓ **Securus has read, understands, and complies.**

SVV automatically assigns, captures, and stores a unique identification number for each video visitation session.

- 2.5.14 System must use set durations of 30 minutes increments for each visit on-site visits

✓ **Securus has read, understands, and complies.**

SVV can be configured to set the duration of visitation sessions to 30 minutes or any increment Maricopa County requires.

- 2.5.15 System duration for online Web to be determined by vendor.

✓ **Securus has read, understands, and complies.**

While Securus' standard visitation session is 20 minutes, we will work with Maricopa County to determine whether a different standard for online visitation sessions is more suitable.

- 2.5.16 Security Levels for Users - The system shall be capable of assigned password access for different levels of security to include System Manager, System Administrator, User Security Level Access by task and location.

- 2.5.16.1 Each user will require a unique username and password that will dictate their level of functionality.

✓ **Securus has read, understands, and complies.**

SVV requires that each user have a unique username and password, which can be tied to different levels of security and functionality.

2.5.16.2 The system provides authorized users the ability to do searches and create reports.

✓ **Securus has read, understands, and complies.**

Users can tap into SVV's robust reporting features to perform myriad searches and create a variety of reports.

2.5.17 Video Searching - The system shall be capable of searching records by Booking number, Inmate name, Visitor name or assigned number, IP address, Visitor ID number, and date/time. Please describe searches available by your system.

✓ **Securus has read, understands, and complies.**

The System currently has the ability to search date/time logs, user names (either inmates or Friends and Family), and Booking numbers. It also has the capability to capture the IP address.

2.5.18 The system shall detect when extra people or voices are present and a notation shall be included in the video detail record of the attempt.

✓ **Securus has read, understands, and does not comply.**

Like all video visitation systems, Securus' SVV does not currently have the ability to detect extra people or voices during the Video Visitation Session. However, Securus is experienced in such technologies and does have the ability to identify registered voices using Voice Biometrics in its Continuous Voice Verification (CVV) product for the Inmate Telephone System. As users of Securus' Inmate Telephone System (SCP), Securus customers avail themselves to the most cutting edge and technologically sophisticated information systems in the industry. These systems will integrate and share information with each other to identify targeted leads, such as our THREADS™ Product.

2.5.19 Attachment of Notes to Video Records - The system shall have the capability of attaching up to six (6) notes of at least 50 characters to any call record to include information such as case number or other investigative data. Describe the process.

✓ **Securus has read, understands, and complies.**

Though this feature is not directly available in our SVV product, the ability to attach notes to SVV session recordings can be accomplished using our proposed THREADS™ investigative tool. Securus is experienced in developing such applications and has developed this feature, which is currently available to users of our inmate telephone system. We are currently in the process of developing and exploring such capabilities in products such as SVV; we continue to develop capabilities for SVV that mirror the capabilities in its inmate telephone system. This ensures continuity of use between SCP and SVV.

- 2.5.20 The system shall provide a visual countdown clock to inform visitor of how much time is left.

✓ **Securus has read, understands, and complies.**

An on-screen timer shows the amount of time remaining for a visitation session.

- 2.5.21 The system shall provide a visual warning message to inform the visitor that the visit will be ending in 2 minutes.

✓ **Securus has read, understands, and complies.**

Securus displays a countdown timer during an entire SVV session so both the visitor and inmate are constantly aware of the time remaining in their visit.

- 2.5.22 The system shall automatically cancel any pending visits if inmate is in-process or has been released from jail.

✓ **Securus has read, understands, and complies.**

Because it is completely integrated with the Jail Management System, SVV automatically cancels any scheduled visit if an inmate is released or transferred to another facility.

- 2.5.23 The system provides a way to display scheduled visits to Staff so they know where and when an inmate needs to be available for pending video visits.

✓ **Securus has read, understands, and complies.**

Staff will use the Video Visitation Dashboard to monitor scheduled visits so inmates can be told when and where their sessions will occur.

- 2.5.24 Authorized personnel must be able to quickly and easily schedule visitation sessions.

✓ **Securus has read, understands, and complies.**

Once authorized to schedule visitation sessions, friends and family members can easily schedule visits by accessing www.securustech.net using any standard Internet browser. This Web site allows users to establish an account, schedule and pay for a video-visitation session, and view account activity.

Authorized Maricopa County Jail personnel can easily schedule sessions using the Video Visitation Dashboard.

- 2.5.25 The scheduling and management system must be able to communicate with the video hardware at the time of a scheduled visit so that the visitation session will automatically commence without staff involvement.

✓ **Securus has read, understands, and complies.**

Staff involvement is not required for sessions to start or end—this can be configured to occur automatically—though authorized staff still have complete control of the system and can monitor, interrupt, or end any session manually should the need arise.

- 2.5.26 The video visitation system must have visitation recording capabilities.

✓ **Securus has read, understands, and complies.**

One of the primary advantages of implementing video visitation is the ability to live monitor and record video visitation sessions. This capability creates new investigative opportunities and also reduces violence within jail walls. In addition, the Securus Video Visitation interface enables jail staff to flag visits for later investigative review and lock recordings from being purged after the standard retention window expires.

- 2.5.27 The kiosk must be able to access the web-based application and be enabled for touch screen inputs.

✓ **Securus has read, understands, and complies.**

SVV terminals are directly connected to the Web-based system and feature hardened glass touch screens for user inputs.



- 2.5.28 The kiosk will provide the inmate with standard information that is retrieved from the facility's jail management system. Standard information would include such things as upcoming court dates, Inmate account balances, and visits.

✓ **Securus has read, understands, and complies.**

SVV's inmate information application allows inmates to retrieve and display court dates, inmate commissary account balances, etc. on the visitation terminal.

- 2.5.29 Provides an audit trail of all system activity (i.e., user login times and locations, which users have scheduled/modified/cancelled a visit, etc.).

✓ **Securus has read, understands, and complies.**

Because all users are required to sign in with their unique username and password, SVV automatically tracks all activities, which can be viewed by administrators at any time.

2.5.30 Additional Features - Describe any additional features available that could be included as part of this proposal.

✓ **Securus has read, understands, and complies.**

JOBview 2nd Chance

Securus has partnered with JOBview 2nd Chance to provide technology that addresses an important issue facing most facilities today—inmate reentry into their communities. One important aspect of successful reentry is the inmate's ability to find a job. The JOBview 2nd Chance solution accelerates this process by putting open job listings securely at the fingertips of inmates.

JOBview 2nd Chance is hardware and software that allows people returning to the community from prisons and jails to search for statewide and nationwide jobs without direct access to the internet. JOBview 2nd Chance is "prison-ready" because the user **does not have access to the Internet**. Job listings are accessed through a secure wireless connection from device to the JOBview data center via a virtual private network. Jobs can only be searched using an interface, which controls and limits what the user can see and do. Job descriptions, along with job application requirements and instructions, can (if allowed by the facility) be printed directly from the device to assist the user with later follow-up. The JOBview program is self-service, requires no user training, and can be enhanced with educators or reentry specialists at your facility.

JOBview 2nd Chance provides non-duplicate access to nearly 1 million job listings. This access contains job listings from virtually all job databases in the United States including CareerBuilder and SnagAJob. The listings are updated daily so users are always searching current jobs. Other versions of JOBview 2nd Chance are available and job listings are updated through a USB or CD media device on a regular basis.

Inmate Benefits:

1. Get a 30-90 day head start on a job search
2. Browse state and nationwide jobs that are current and updated nightly
3. Start thinking about jobs before release; putting their mind on something positive
4. See what skills and specific requirements they will face well ahead of release
5. Match educational programs to the types of jobs they qualify for and will encounter
6. Practice electronic job searching which is technology they will commonly see upon release
7. Job listings of interest can be printed and used for reference after a kiosk session

Correctional Facility Benefits:

1. No incremental job-seeker training costs because the user interface is self-explanatory
2. Staff no longer needs to find and print job listings for their transitioning inmates
3. Job listings are available for all types of jobs and levels of experience in cities nationwide
4. Turnkey service; JOBview (or Securus) takes care of everything
5. No long-term contracts with other vendors;
6. The annual cost of the JOBview service is paid for by Securus

As stated, there are multiple product(s) which are available depending on the security requirements of the facility.

JOBview 2nd Chance Non-Apply VPN: Users can search for jobs but they cannot apply. The device is configured with a wireless connection to the JOBview datacenter over a virtual private network (VPN). The VPN only allows the device to access updated job listing data at the JOBview datacenter. The user has no access to the internet.

JOBview 2nd Chance Non-Apply JOBswap: Users can search for jobs but they cannot apply. The device is a stand-alone configuration with no wireless connection to the JOBview datacenter. The jobs database is updated from a JOBswap media device (USB or CD) provided to the facility monthly, or more often if desired. The update process is fully automated once the media device is inserted into the device which allows inmates to search for jobs from prison.

A Software Only version of JOBview 2nd Chance: Is also available for installation on Windows-based computers or servers in your facility. If you can provide a secure connection (through a proxy) to the JOBview datacenter, inmates will be able to search our "live" jobs database but they will not be able to apply. If the computers do not have access to the internet, the jobs database is updated from a USB or CD media device provided monthly, or more often if desired.

PHD Medical Televisit™

In addition to SVV's many features, Securus also can provide the optional PHD Medical Televisit™ telemedicine solution to help Maricopa County realize a variety of efficiencies and increase your public safety. By using the Televisit system, Maricopa County can reduce the amount of external inmate transports, thereby reducing staffing costs and increasing public safety. Televisit provides facilities with the ability to perform routine evaluations, specialty consultations, and emergency medical examinations without the need to transport inmates. All session information is stored in the TeleVisit EMR that can be exported to other electronic medical records (EMRs) or printed for use in paper files.

Why PHD Medical?

With an aging incarcerated population, unprecedented budgetary pressure, and public safety concerns, it is imperative to have contracted medical providers at the ready to reduce the transportation of inmates. To maintain a balance between quality of service and budgetary constraints the use of communication technology, such as TeleVisit, is a necessity. Televisit expands your clinical reach and provides a tool to recruit and/or expand your clinical network of professionals. Televisit is an **FDA approved** telemedicine suite that has been specifically built to

integrate with a host of medical devices required for your medical examinations. These devices are all controlled by the remote doctor; therefore your facility staff requires minimal training on the TeleVisit technology. With Televisit at your facility you can have on-demand access to the clinical resources you need; when you need them.

How can it help Maricopa County?

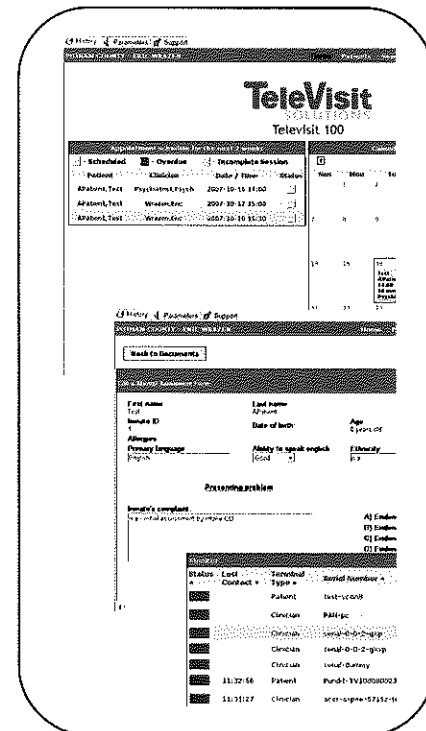
Stop transporting inmates and start using Televisit to see these immediate benefits:

- Carry out daily scheduled health clinics for hypertension, diabetes management, etc.
- Perform psychological evaluations and clinical sessions for other mental health issues
- Use the suite of medical devices to perform exams with specialists such as dermatology, Neurology, Cardiology, etc.
- Perform emergency examinations to determine whether the patient should be moved to an outside facility for care
- Track the health of inmates using the built in medical records system, which allows you to manage existing conditions, adjust prescription regimens, and report on outcomes

Key Features

Maricopa County can take advantage of many of TeleVisit's features, which help identify it as a premier tool in providing quality health care for your inmates. These features include the following:

- **Medical Grade:** The Televisit Cart is built using hospital grade equipment and has a built in UPS that allows the cart to be used untethered for greater than six hours per day.
- All software and medical devices are **FDA approved**.
- **Devices:** Inmates can be examined with the medical devices built into the Televisit Cart, such as a blood pressure monitor, oximeter, otoscope, thermometer, hand held proscop (for wound and skin examination), stethoscope, glucometer, scale, EKG, and a powerful pan/tilt/zoom camera with 10X optical zoom. We are regularly integrating more medical devices to the system for future use.
- **Electronic Medical Record:** Televisit provides a simple EMR that can be used to store and track patient information and data. This information conforms to HL7 standards and can be easily exported to more robust systems.
- **Scheduling and Management System:** Using the built-in interfaces, users can easily schedule appointments, review the results of examinations,



Scheduling and Management Interface

and manage user accounts and access.

Benefits

Televisit is the only FDA approved telemedicine solution that allows users to schedule, perform and report on real-time consultations. With TeleVisit you've got the tools needed to provide exceptional healthcare while controlling your budget and keeping public safety concerns at bay.

Automated Information Services

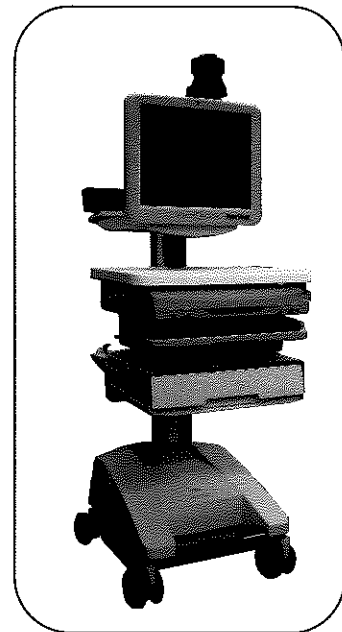
Our proposed SCP solution for Maricopa County offers the industry's first and only hosted interactive voice response (IVR) system: AIS™. Securus has partnered with Telerus as the exclusive provider of AIS. Securus will provide AIS to Maricopa County and provide this service for use by both the public and inmates. AIS can be offered as a minimum non-commissionable surcharge on the inmate phone calls without raising rates to constituents or as a slight commission deduction, whichever the county prefers. AIS automatically provides general facility and inmate-specific information to detainees and outside callers over the phone. Automation of the repetitive questions asked by inmates greatly reduces the workload on officers, allowing for reallocation of that time to more important command and control functions.

AIS provides inmates and outside callers with the ability to access inmate-specific and general facility information over the phone. Inmates are able to access the system by dialing a speed dial on any designated inmate phone, while outside callers access the system by dialing the main facility telephone number. AIS is hosted through the SCP centralized architecture and will use the existing telephones number.

In addition to this core functionality, AIS can be configured to allow friends and family to open or fund a prepaid telephone account as well as fund an inmate's trust account over the phone. These additional funding options make it easier and more convenient for friends and family to contribute funds while increasing your facilities potential commissionable revenue. All of this functionality is automatically available around the clock, which means constituents will always be able to get the information they need when they need it.

AIS can automate information, such as the following:

- Criminal charges
- Bond amounts and types
- Court dates, times, and locations
- Projected release date
- Commissary balance
- Visitation eligibility



- General facility information
 - Facility location
 - Directions
 - Hours
 - Mailing policies
 - Visitation policies
 - Money deposit policies

AIS provides unmatched secure access into facility and inmate information. This information is pulled from a facility's various management information systems including your Tiberon JMS and court systems every 15 minutes.

The service offers an English and Spanish interface, text-to-speech playback of inmate names, and touchtone and speech recognition interface. Friends and family access AIS by calling into your normal telephone number while inmates access their information by simply dialing a speed dial from any inmate telephone.

By implementing AIS, you will...

- Improve the efficiency of your facility—*Gain satisfied inmates and friends and family while reducing the workload on your staff to focus on other responsibilities*
- Use the phone system you already installed—*no need for additional hardware or wiring*
- Answer 90 percent of inmate questions now made to correction officers
- Reduce constituent calls to your facility between 80 and 90 percent—*automated system provides 24 hour access that eliminates the most common calls*
- Realize a 200 percent increase in “answered” calls—*constituents who traditionally hang up because of extended wait times are much happier*
- Gain a reliable system that has a 99.9 percent uptime service level agreement
- Receive a Usage Summary automatically e-mailed to your facility monthly
- Increase your commissionable revenue by opening up another method for funds flowing into your facility

AIS Return on Investment

Most detention facilities find incoming phone calls to be an enormous administrative burden. In fact, Securus has found that an average facility receives one-half phone call per day per inmate and each call averages a duration of four minutes. We have also found that inmates ask facility personnel one-half question per day. Not only do these activities results in higher consumption of administrative resources, but they take facility personnel away from their primary job responsibilities.

Monthly Time Consumption per Inmate

1 inmate x ½ call x 4 min x 30 days = 60 minutes

AIS Value

- Incoming Requests: AIS automates 80 percent of administration requests, which results in a savings of 48 minutes per ADP per month
- Inmate Requests: AIS automates 90 percent of inmate requests, which results in a savings of 54 minutes per month per ADP

AIS saves facilities time, money, and helps better serve constituents. Automating both friends and family member and inmate requests enables facility personnel to focus on their primary responsibilities.

Weld County has AIS for both the inmates and the public. AIS automates 86 percent of the public calls every month. In addition, AIS has received more than 13,000 inmate calls for bond information, court dates, projected release dates, etc. over the last six months. AIS has been used by the inmates during this six-month time frame 298 hours!

Testimonials

"Automated Information Service, AIS is a product my staff could not live without. The amount of time that AIS saves my staff on their day to day operations is invaluable. Staff is no longer bombarded with questions from inmates in regards to outdates, fund balances in accounts and court dates. The number of grievances has dropped significantly since implementing AIS on the inmate side."

- Captain Gary Gittins, Jefferson County Detention Center

"Someone came back from vacation just after AIS was installed and reported that there was a problem with the phones because they weren't ringing anymore."

- Lt. Hammond, Lorain County

"Our deputies love it, so I love it. We're now saving over two officer's worth of time!"

- Dee Sandy, Miami County

The following graphics depict sample AIS Caller Reports covering a four-month period for calls from the public (outside the facility) and from inmates, respectively.

Sample AIS Caller Report

PUBLIC USAGE	
CALLS	
Total Calls	43460
Forced Transfers	7808
Automation Rate	82.03%
Total Call Duration	67944 mins 2 sec (1132 hrs 24 mins)
Average Call Duration	1 mins 33 sec
Phone Account Funding Selected	4828
MENUS	
Main Menu Played	43446
General Info Menu Played	2851
Inmate Specific Menu Played	52078
LANGUAGE	
English Callers	41232
Spanish Callers	2228
INMATE LOOKUP	
Inmate Lookup Prompt Played	38847
Inmate Name Confirmed	18312
Inmate Birth Date Confirmed	2215
INMATE SPECIFIC	
Charges Played	7884
Bail Bond Info Played	7191
Projected Release Date Played	8178
Next Court Date Played	8564
Visitation Schedule Played	4644
Inmate ID Played	2326

INMATE USAGE	
CALLS	
Total Calls	105048
Total Call Duration	99381 mins 8 sec (1656 hrs 21 mins)
Average Call Duration	0 mins 56 sec
MENUS	
Main Menu Played	242074
LANGUAGE	
English Callers	87353
Spanish Callers	9613
INMATE SPECIFIC	
Commissary balance Played	88841
Charges Played	10516
Bail Bond Info Played	11726
Projected Release Date Played	13617
Next Court Date Played	33005

Inmate Information

Along with AIS is SVV's Inmate Information module. Very briefly, the Inmate Information application allows inmates to retrieve inmate specific information and display on the visitation terminal. This information may include commissary balance, scheduled court dates, etc.

Sick Form

The Sick Form allows inmates to document and submit symptoms of illnesses. Administrators will then be able to view submitted forms and take necessary action regarding the appropriate medical care for infirmed inmates.

Additional Future Capabilities

Our R&D staff actively works to meet the emerging and evolving needs of our customers as the use of this technology matures. We seek input from our customers to learn the market-driven needs that will help craft the future of video visitation. As an important Securus customer, when Maricopa County identifies a new, high-demand need for the system, you most likely will see it in a future release.

As we look to the future of video visitation, Securus has evaluated such uses as paid secure Internet browsing, paid games, law library access, and music/MP3 sales using the Securus Video Visitation terminals.

2.6 PHASE 2 - INMATE RULES AND REGULATIONS REQUIREMENTS

Estimated implementation duration: 1 month

- 2.6.1 The complete Rules and Regulations for Inmates will be available electronically on the kiosk. Inmates will be required to acknowledge the availability of these rules and regulations with an electronic signature when they establish their Personal Identification Number.

✓ **Securus has read, understands, and complies.**

Currently under development, SVV will be capable of enabling inmates to read documents such as MCSO's Rules and Regulations on the terminal. Inmates will be required to access the documents using unique PINs, which will be used to verify and acknowledge that they have read any required documents.

- 2.6.2 If an inmate who is still in custody after 48 hours from the time they are accepted into custody and they have not yet acknowledged the availability of the Rules and Regulations for Inmates on the kiosk, an electronic message will be forwarded to the commander of the Bureau Hearing Unit, or his designee, for appropriate follow-up.

✓ **Securus has read, understands, and complies.**

Securus is considering this capability but has not yet scheduled it for our development road map. As a functional equivalent and until it is firmly identified as an enhancement to SVV, Securus system administrators will generate compliance reports required by Maricopa County to provide this capability without additional work for the County.

2.7 PHASE 3 - INMATE FORMS REQUIREMENTS - TANK ORDERS & LEGAL REQUESTS

Estimated implementation duration: 2 months

- 2.7.1 The inmate will complete tank orders and legal requests via touch screen keyboard and be signed for by using signature screen without using a light-pen or other attachment.

✓ **Securus has read, understands, and complies.**

SVV terminals have a touch screen keyboard function that can be adapted for use with Maricopa County's tank orders and other forms. The terminals do not require and do not have a light pen or other external attachment.

2.7.1.1 The forms shall be automatically routed to the appropriate locations where they can be processed.

✓ **Securus has read, understands, and complies.**

SVV is currently configured to route forms to a queue that can be accessed based on one of three groups authorized users are granted security permissions to. Securus is willing to work with Maricopa County to better understand your needs in this area and develop such routing capabilities.

2.8 PHASE 4 -INMATE CANTEEN REQUIRMENTS

Estimated implementation duration: 3 - 6 months

2.8.1 The kiosk will provide for commissary ordering with real-time account balance via touch screen inputs.

✓ **Securus has read, understands, and complies.**

Securus will interface SVV with Maricopa County's commissary ordering system to display account balances that will be updated based on the refresh cycle established between the two systems. Real-time updates can be made though they would have to be initiated from the commissary system.

2.8.1.1 Commissary application shall have pictures of products.

✓ **Securus has read, understands, and complies.**

SVV will display pictures of products in Maricopa County's commissary.

2.8.1.2 Commissary application shall make it known if product is not available.

✓ **Securus has read, understands, and complies.**

Commissary items that are out of stock and not available can be denoted on the SVV terminals.

2.9 PHASE 5 - INMATE FORMS REQUIREMENTS - GRIEVANCES AND APPEALS

Estimated implementation duration: 2 months

2.9.1 The inmate will complete grievance and appeal forms via touch screen keyboard and be signed for by using signature screen without using a light-pen or other attachment.

✓ **Securus has read, understands, and complies.**

SVV's Grievance Module is a two-way communication vehicle between inmates and the facility and will be acknowledged by the inmate by either accepting or rejecting the facility's grievance response.

2.4.29.1 The forms shall be automatically routed to the appropriate locations where they can be processed.

✓ **Securus has read, understands, and complies.**

SVV is currently configured to route forms to a queue that can be accessed based on one of three groups authorized users are granted security permissions to. Securus is willing to work with Maricopa County to better understand your needs in this area and develop such routing capabilities.

2.10 PHASE 6 - INMATE E-MAIL REQUIREMENTS

Estimated implementation duration: 4 months

2.10.1 The kiosk will provide an Inmate Email solution.

✓ **Securus has read, understands, and complies.**

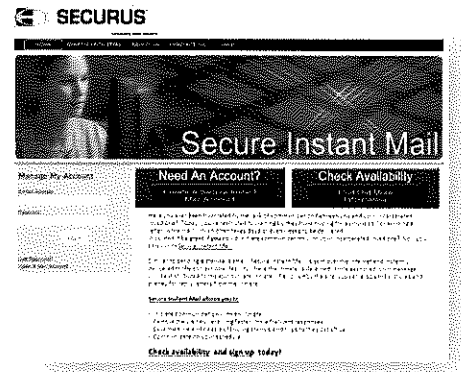
Securus proposes to operate its Secure Instant Mail (SIM) application on the SVV terminal, giving inmates another way to communicate with friends and family and Maricopa County both an additional source of revenue and a tool that investigators can use to solve crimes.

SIM enables friends and family members to establish a prepaid email account with Securus to securely send and receive email messages to inmates. These prepaid email transactions **are commissionable, adding an incremental source of revenue to Maricopa County**. SIM was designed to take facilities:

From...	To...
A manual mail process	✓ An automated email process
No revenue related to inmate mail	✓ Increased facility revenue through emails
Limited investigative capabilities	✓ Archived, searchable email database
Potential mailed contraband risks	✓ No mailed contraband physically possible
Labor intensive mail security	✓ Increased security through automation
Limited visibility of inmate mail traffic	✓ Interactive email activity dashboard
Facility staff dedicated to a mail room	✓ Anytime, anywhere email review and approval process from laptops or even smart phones
Standard sort and deliver mail method	✓ Flexible mail options designed to work with facilities' unique needs

Secure Instant Mail also considers the communication needs of inmates' friend and family members in Maricopa County communities, enabling them to:

- Access a simple email interface, designed to look and feel like other public email clients.
- Initiate the communication with the inmate to send and receive emails and even pictures—*anytime, anywhere*.
- Gain peace of mind, knowing the inmate received the mail by viewing approved email delivery receipts.
- Communicate more frequently without the need of stamps, envelopes, and on their schedule.



How It Works

Secure Instant Mail is similar to standard email but built for the corrections environment, meaning it was designed to be flexible, secure, efficient —and profitable for the county.

1. Account Setup and Sending Email

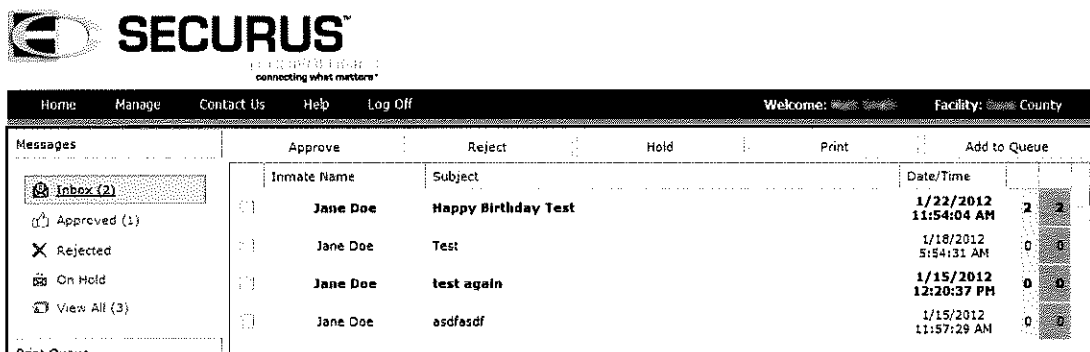
The inmate's friend or family member sets up a Secure Instant Mail account by going to www.securustech.net. Using the Secure Instant Mail website, they can select the facility and inmate receiving the email, compose the email, select messaging options, pay for the email and send the email. Messaging options include requesting approval notifications, prepaying for inmate responses, and even uploading pictures. The email is then processed through the system for the facility's approval before it is sent to the inmate.

2. Facility Approval

Authorized facility staff logs into the facility's Secure Instant Mail website with a secure user name and password to manage inmate emails. Staff can review, approve, and reject emails and pictures. This process is simplified through a customizable **automatic word search engine**, which flags illicit and potentially illicit words in the emails.

The following figure illustrates the system's capability to flag pending emails that contain word warnings. Their critical relevance is indicated as "red" or "yellow." The facility staff can easily point and click for approval or rejection from any approved PC at anytime, anywhere.

Secure Instant Mail Inbox with Red and Yellow Warning Word Indicator



Once the email is approved, it is archived and can be distributed to the inmate. If the friend or family member has selected to be notified, they would receive an automatic reply email at this time, confirming the approval.

3. Delivery to the Inmate

Maricopa County inmates will receive the email through optional methods including print format and by accessing a Securus Video Visitation kiosk (if available in the facility). Inmates may reply to their email through kiosks or by submitting their written response to facility staff to be approved and scanned into the system to be sent via email to the friend or family member.

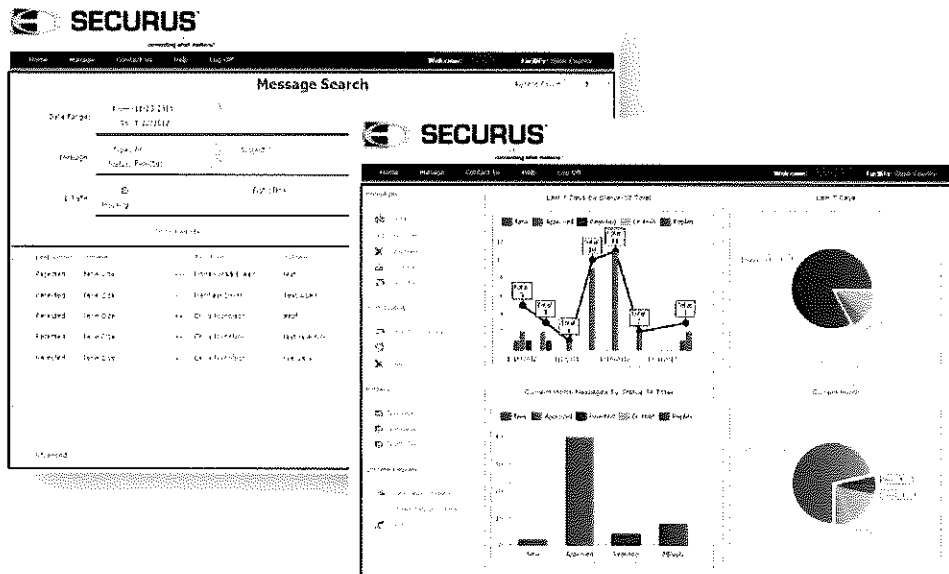
Improving Maricopa County Operations Through Automation and Innovation

Secure Instant Mail was not only designed to provide Maricopa County with additional revenue, but also to improve mail room operations security and efficiency. This is accomplished through fully integrated technology that places all automated tools needed to create, approve, send, and receive, and respond to email in the hands of the users.

Use of Secure Instant Mail includes the following benefits:

- Eliminates the need to open, analyze, sort, translate, or x-ray mail.
- Reduces contraband, improving the safety of facility officers as well as inmates.
- Speeds up the emails approval process through integrated word search engine with a built-in, editable dictionary.
- Enhances investigations by archiving each email in a secure centralized database. Through the Secure Instant Mail website, investigators can search for emails by inmate, sender, date range, keyword, and much more.
- Provides an interactive dashboard of email traffic by type, status, and date—*giving administrators a complete email management tool right at their fingertips.*

Secure Instant Mail Message Search and Interactive Dashboard



- 2.10.1.1 Inmates will be able to receive an email from an approved user that pays and prepays for response. Emails shall be no more than 500 characters in length.

✓ **Securus has read, understands, and complies.**

SIM is configurable to limit emails to 500 characters. Securus default is 6,000 characters, so should Maricopa County revise this specification it can likely be accommodated.

- 2.10.1.2 The email system shall have a word recognition program that can identify certain words, phrases, or slang and flag it.

✓ **Securus has read, understands, and complies.**

SIM enhances investigations by archiving each email in a secure centralized database. Through the SIM Web site, investigators can search for emails by keyword, inmate, sender, date range, and much more.

2.11 PHASE 7 - CORRECTIONAL HEALTH SERVICES REQUIREMENTS - HEALTH CARE NEEDS FORMS

Estimated implementation duration: 2 months

✓ **Securus has read, understands, and complies.**

2.11.1 The inmate will complete Health Care Needs Requests via touch screen keyboard and be signed for by using signature screen without using a light-pen or other attachment.

✓ **Securus has read, understands, and complies.**

SVV terminals will not feature any external attachments, such as a light pen, but rather will use the terminals hardened touch screen features and PINs either separately or in combination to verify user functions.

2.11.1.1 The forms shall be automatically routed to the appropriate locations where they can be processed.

✓ **Securus has read, understands, and complies.**

SVV can be set up to allow only medical staff to see the requests and print them out for follow up.

2.11.2 The kiosk will provide for sick call reporting via touch screen inputs.

✓ **Securus has read, understands, and complies.**

The Sick Form allows inmates to document and submit illnesses. Administrators will then be able to view submitted forms and take necessary action.

2.12 FUTURE DOCUMENTS AND APPLICATIONS

2.12.1 The system will include the capability to add additional document applications and/or upgrade previously installed documents and applications as necessary.

✓ **Securus has read, understands, and complies.**

The Securus system is designed to add additional applications and/or upgrade existing applications over the term of the agreement. Our system is designed to evolve and provide enhancements as new needs are uncovered.

3.0 INTERFACE REQUIREMENTS

The proposed system must interface with MCSO data systems using MCSO-preferred transaction-oriented protocols in near real-time within our secure network environment. The preferred approach is via a vendor centralized server connection to the County Integration Engine to minimize external connectivity to the MCSO network. The County Integration Engine is used to facilitate connectivity between systems using a myriad of transport and data formatting protocols. The County Integration Engine uses IBM WebSphere MQ messaging as the preferred transport for guaranteed store-and-forward delivery. In this configuration, the County's MQ messaging server would host connections to the vendor system, which would run MQ client software.

Additionally, MCSO maintains a full, parallel development/test environment for IT systems. Vendor systems should integrate with existing MCSO systems and processes and should support a full development/test environment. Please elaborate on how your proposal will meet or exceed these requirements.

For the initial implementation of the web-based video visitation system (WVVS) a small set of transactions should be implemented to help coordinate the scheduling of inmates for visits. The Jail Management System (JMS) holds the schedule for all inmates' time commitments. System integration transactions between the WVVS and the JMS should be created to help coordinate the scheduling of inmate video visits. As an example, there should be a transaction sent by the WVVS to the JMS requesting a list of scheduled appointments for a given time period (one day or more). With the JMS response the WVVS would be able to determine and display available time slots for visitation.

✓ **Securus has read, understands, and complies.**

Maricopa County will be in full control of all scheduling of visitation sessions within SVV. Securus currently use flat files and web services for all integrations but we can develop this new method using WebSphere MQ messaging.

Securus Dedicated Integration Team

Securus has solid, proven experience with Integration. Securus currently integrates with more than 110 different vendors worldwide and over 60 independent facility owned systems/shared databases.

Securus has its own dedicated Integration Department that works exclusively on integrating the various systems and products in the correctional environment. Having this dedicated Integration Department allows Securus to deliver fast and flexible solutions for our customers. Securus' technology is flexible and does not mandate rigid specifications when working with facility owned systems, JMS, OMS, Commissary, Banking, and Kiosk vendors, etc. Securus will fully cooperate with your facility and your vendors to automate the systems.

The most common technologies Securus uses to integrate with your systems include: SOAP Web Services, HTTP, FTP push or pull of files in any textual format, JSON, XML-RPC, and TCP Sockets. All of these methods are performed over a secure connection.

Securus is able to transform your data format for insertion into our platform, negating the need for costly code modifications to your system. Securus integration engineers will consult with your

facilities IT department or system provider to determine the best integration strategy for your specific application.

Securus Integration Process

The dedicated Securus Integration team is our dedicated group of individuals that designs, develops, tests, and implements all custom integrations with corrections industry and banking systems. Our mission is to deliver fast and flexible solutions for our customers. This process is incorporated into the overall Project Plan for the installation of the Securus SCP inmate telephone system. Major milestones include:

- Collect Preliminary Needs/Requirements
- Contract Signed
- Finalized Requirements document
- Approved Scope Statement
- Finalize Design Document
- Schedule Customer Implementation
- Develop Custom Integration Solution
- Test Custom Integration Solution
- Implement Custom Integration Solution
- Customer Approval and Sign off

Development/Testing

Securus will integrate with existing MCSO systems and processes and to support a full development/test environment. Securus supports and utilizes today a four level IT environment today:

- Development
- Quality Assurance
- Pre-Production
- Production

Scheduling of Inmates' Time Commitments

SVV schedules based on information from its most-recent JMS data feed. When an inmate is registered in JMS as being unavailable for whatever reason, any video visitation sessions for that inmate in that time period are automatically cancelled by the system. For example, if a video visitation session is scheduled from an inmate at 10 a.m. on a Monday morning but the inmate is moved to the infirmary at 9 a.m., when SVV receives that data it will automatically cancel that session and issue a credit for the session to the visitor, who can reschedule at their convenience.

4.0 NETWORK:

- 4.1 Active network and associated equipment shall be owned and maintained by MCSO. This equipment and interconnections shall be purchased by the vendor, as per our specifications, as part of the "no cost" initiative. The active network equipment will be composed of Cisco router and switch devices, which will be interconnected site-to-site via Metropolitan Optical Ethernet circuits. These network devices shall be configured for use by the vendor to insure proper compatibility with their end devices.

✓ **Securus has read, understands, and complies.**

Because of the high bandwidth demands for the SVV system's network requirements, Securus proposes to operate the system on a separate, parallel network that will offer equivalent or higher levels of service than from piggy-backing on MCSO's network. While MCSO will own the network that Securus procures and installs, operating it separately will maximize efficiencies of both networks because of the resource demands of transmitting audio and video signals. Securus will configure and install network devices are both compatible with end devices and will optimize network functionality.

- 4.1.1 The video visitation system shall be a complete IP-based system. All video and audio streams between the terminals, visitors, and management equipment (servers) shall be transmitted over Ethernet.

✓ **Securus has read, understands, and complies.**

- 4.1.2 Systems that utilize analog audio/video matrix switching systems are not acceptable.

✓ **Securus has read, understands, and complies.**

SVV is fully Web based and digital, and does not have analog components. It is a centralized system that allows automatic technology and feature upgrades. After the video visitation system has been implemented, it is easy for Securus to enable new features and modules by activating the feature in the centralized system.

- 4.1.3 The video visitation solution shall consist of inmate kiosks connected over a 1Gbps local, dedicated Ethernet network. Each site shall be connected to other sites via a 50Mbps CenturyLink Metropolitan Optical Ethernet circuit. These MOE circuits shall reside in a private cloud through CenturyLink.

✓ **Securus has read, understands, and complies.**

Securus will provision and implement the network SVV operates on and ensure that it includes sufficient bandwidth to meet the visitation needs of Maricopa County, your inmates and their friends and families. Securus will upgrade the network and VVS as necessary during the life of the agreement.

- 4.1.4 The visitor terminal shall be able to access the video visitation solution via local area network (LAN) and via a broadband internet connection (DSL, cable, etc.) using a computer or laptop that is web camera and headset enabled.

✓ **Securus has read, understands, and complies.**

- 4.1.5 High quality video using low bandwidth

✓ **Securus has read, understands, and complies.**

- 4.1.6 Video Standards: H.264

✓ **Securus has read, understands, and complies.**

- 4.1.7 Video Transmission Speeds: 64 Kbps - 2 Mbps

✓ **Securus has read, understands, and complies.**

- 4.1.8 Wide range of video resolutions and bit rates: CIF (352 x 288 pixels), SIF (352 x 240 pixels), QCIF (176 x 144 pixels)

✓ **Securus has read, understands, and complies.**

- 4.1.9 Constant or variable bit rate and frame rate

✓ **Securus has read, understands, and complies.**

- 4.1.10 Must provide encryption for all visits

✓ **Securus has read, understands, and complies.**

Securus encrypts all video visits using 128 bit encryption to ensure visitation traffic is kept private and secure as it travels over the Internet.

- 4.1.11 Please describe the expected network traffic or bandwidth usage requirements of your system.

✓ **Securus has read, understands, and complies.**

Securus will provide the network that SVV will operate on and provision it to run in the most efficient manner possible. Each video session transmits and receives data at a throughput rate of ~250kbs.

4.2 CABLE/ELECTRICAL POWER:

- 4.2.1 The Contractor shall be responsible for the installation of all necessary low voltage CAT6 cable, power lines, electrical hookups, for each video kiosk with control in each facility.

✓ **Securus has read, understands, and complies.**

Securus will be responsible for all installation activities except for approvals by Maricopa County.

- 4.2.2 Existing house cable used to provide services becomes the property of MCSO.

✓ **Securus has read, understands, and complies.**

Per discussion during the pre-bid conference, Securus will replace all existing cable on Maricopa County's current video visitation systems with new CAT6 cable.

- 4.2.3 Any electrical work shall be coordinated through Maricopa County Facilities Management Department, using their list of contracted vendors for completion of this type of work. Low voltage CAT6 cabling shall be coordinated through MCSO Telecommunications staff, using the on-site contracted vendor.

✓ **Securus has read, understands, and complies.**

Securus will coordinate with Maricopa County Facilities Management Department to contract with a vendor from your approved list. Securus supports efforts to award work to local vendors that are vetted to work in your facility.

- 4.2.4 Power, Grounding and Cooling Requirements - Please describe the power and BTU requirements of your system.

✓ **Securus has read, understands, and complies.**

SVV terminals have the following environmental requirements:

- Operating temperature range: -4 °F to 122 °F (-20 °C to 50 °C)
- Power: 110V, 2.5 amps
- Grounding: All terminals require a three-prong grounded power outlet
- BTU: Each terminal generates approximately 210 BTUs during a visitation session with the lights operating.

4.3 INVESTIGATIVE TOOLS/INTELLIGENCE GATHERING:

The system shall have the ability to provide investigative tools, features, and creative solutions that would enhance MCSO's capability to actively monitor and data mine criminal activity being conducted by inmates in the jails through the Web-Based Video Visitation/Communication Kiosk System. The Contractor's recommendation must be proven technology.

✓ **Securus has read, understands, and complies.**

As an option, Securus can provide Maricopa County with our new, powerful investigative software called THREADS™, exclusive to Securus and not available from any other provider. THREADS will enable Maricopa County investigators mine intelligence data like never before and uncover criminal associations quicker and more efficiently, such as interfacing with TouchPay kiosks to follow the money trail of who made deposits or paid for video sessions and associating that information with other investigative data.

"Major intelligence failures are usually caused by failures of analysis, not failures of collection."

- Richard Heuer Jr., CIA Analyst and Author of *Psychology of Intelligence Analysis*

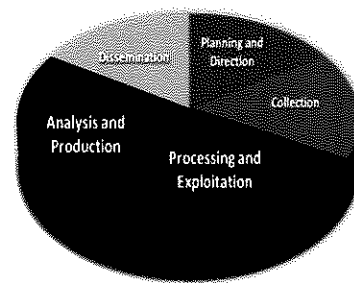
Securus understands the lifecycle of intelligence and investigating communications data and the challenges investigators, detectives, and corrections facility staff face in both time and resources, such as the following:

- Pulling reports
- Exporting information
- Sending information to someone else
- Contacting other facilities for information
- Combining all the information together
- Receiving information in many different formats

- The daunting task of identifying suspicious behavior in the information provided to uncover focused leads

Even when key information is gathered, investigators have to determine where all of the data will go as well as the time consuming method of analysis.

- What if you had a 24x7 analyst that you didn't have to provide a salary or benefits to?
- How much time and money would be saved?
- What if you had a sense of liability protection knowing access to the data is controlled, logged, tracked, and available to only authorized users?



The Securus THREADS product provides the means to answer these questions. The unique algorithms used within THREADS were designed by real investigators with many years of experience analyzing communications data and training other investigative units on how to analyze data.

Managing Investigative Data

Securus understands that during the course of an investigation, the law enforcement community is inundated with data. Data is coming from different sources in different formats with numerous potential leads that can be followed. Each lead potentially creates many more leads to be followed.

We understand investigators are quickly overwhelmed with the amount of information they must analyze as well as the time and resources required to manage, retrieve, and analyze the data to identify those leads that are most likely to uncover important information.

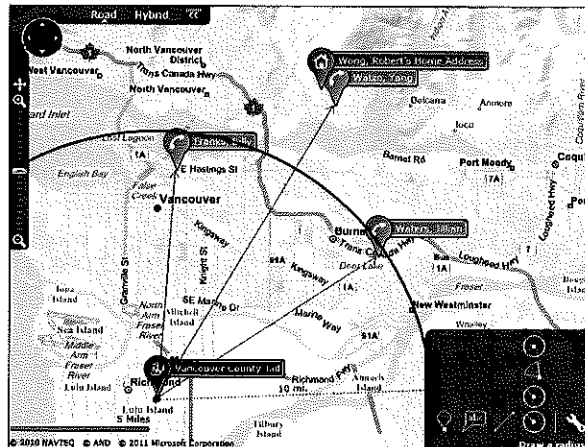
Sources of Information

Corrections Data	External Data
<ul style="list-style-type: none"> • Inmate call records • Inmate personal information (such as name, account number, PIN, DOB, and SSN) • Who the inmate is allowed to call versus who is actually called • Called party billing name and address information • Public phone records 	<ul style="list-style-type: none"> • Confiscated cell phones (such as calls, text messages, emails, videos, and contacts) • Corrections facility information in proximity to calling behaviors • Events and places of interest • Mail • Lexus Nexus • SS7 information

All corrections data (such as call records, phone numbers, billing name and address) is automatically and fully integrated with THREADS the moment THREADS is enabled. All other sources of data are imported into THREADS and analyzed together to automatically build an investigation.

For example, THREADS will uncover calling patterns that lead to a high probability an inmate has a cell phone. That cell phone is confiscated and the information pulled from it using a Cellebrite UFED device or similar tool. This information is uploaded into THREADS, and all that valuable data is analyzed along with the corrections communication data to uncover an inmate's plot to escape or run an organized crime syndicate from inside the facility.

After determining a suspect on the outside of the facility is involved and mapping out the address, the investigator acquires the public phone records and imports that information into THREADS, which is again analyzed with all the other gathered information. This all takes place in one location, with one tool, and is completely integrated with inmate data.

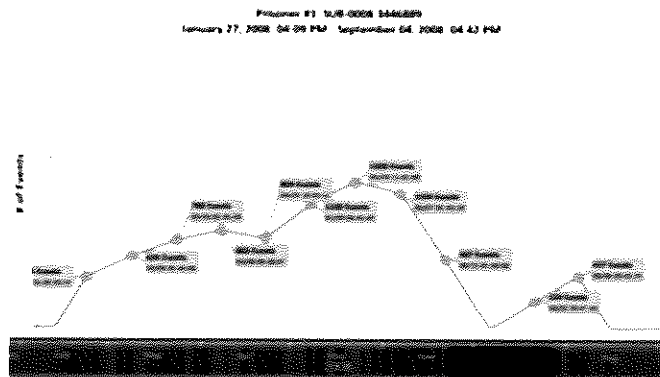


Securus' SCP is the most widely used platform in the industry, with approximately 1,700 facilities installed, more than 850,000 inmates served, literally petabytes of intelligence data, and in excess of 1 million calls processed per day. This valuable data is integrated directly into THREADS and could be available at Maricopa County's fingertips.

Powerful, Accurate, Easy to Use

THREADS is a powerful, accurate, easy-to-use, intuitive tool that will automatically analyze investigative data such as inmate communication records, public phone records, and data from confiscated cell phones to automatically generate focused leads for investigators. Leads can include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple inmates, their correlation to called parties, and much more.

Additionally, this powerful software provides dayroom-based analysis that discovers leads irrespective of the PIN being used by the inmate and common contact reporting showing inmates who are facilitating communications between different areas of the institution. Maricopa County investigative staff can



easily uncover patterns of fraternization between inmates and correctional officers, discover common contacts between inmates and called parties, and customize the information and reporting to filter out irrelevant calls such as to girlfriends or legal counsel from analysis.

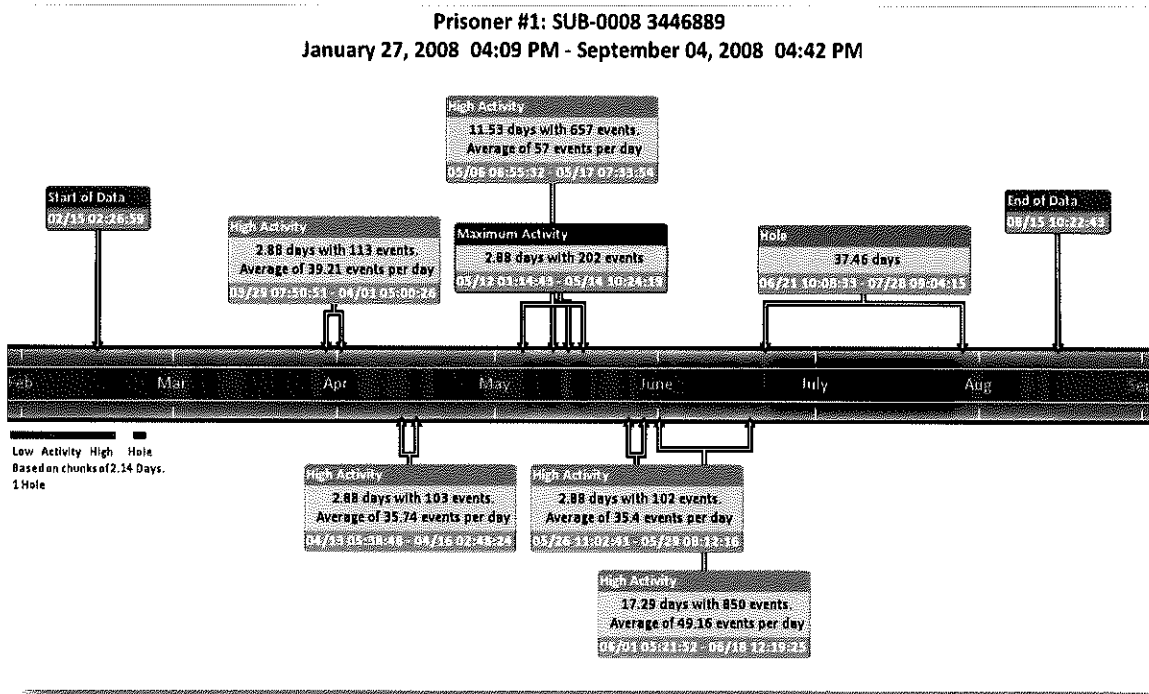
THREADS will detect criminal organizations being run from within jail, detect three-way calling patterns when multiple inmates are talking to one called party at the same time, find associations of multiple called parties based on who is calling them, and identify inmates who possibly have a cell phone based on calling patterns. For instance, if an inmate makes six calls per day, every day, but then all of a sudden doesn't make any for a week, it is possible they have another way to communicate, such as a cell phone.

Graphic Representation

All information is presented graphically as well as textually such as the example presented in the following figure.

Activity and Hole Detection

Proprietary and Confidential



Timeline charts and graphical analysis make it easy to show periods of high-intensity calling and other calling patterns on a graphical and interactive timeline. This technology identifies the inmate even if the calls are masked by another inmate's PIN and eliminates the human intervention by receiving actionable intelligence at the push of a button. Additionally, THREADS allows you to set up automated notifications, which will email an investigator when information is found.

THREADS analyzes data for investigators and provides interactive visualization tools to produce easy-to-understand analytical reports, charts, interactive graphs, maps, and builds a case and presentation view that can be used as evidence in a criminal trial.

Investigative Benefits for Maricopa County

- Cell phone forensics analysis
- Identify accomplices
- Inmates contact people on the outside indirectly, identify who they are “really” contacting
- Identify linkages
- Identify an inmate’s inner circle
- Identify associated gang members
- Identify an inmate’s communications within jail
- Find unique patterns in communications data
- Combine all the data into a single system to analyze
- Harvest all of this information with enhanced reporting tools

Securus’ THREADS is an exclusive investigative technology that no other provider can offer to the correctional industry. THREADS will be available as an optional product and empowers Maricopa County with the latest in investigative technology and one of the most powerful investigative tools in the intelligence community.

Not all investigative capabilities are the same across the industry. Securus is the only company that can offer the THREADS analytical software. THREADS is currently used by the United States Border Patrol, the Department of State, the Department of Defense Cyber Crime Center, the United States Drug Enforcement Center, the Department of Homeland Security, and the U.S. Army—THREADS can be fully integrated into the MCSO’s suite of investigative systems.

- 4.3.1 Random Monitoring of Live Video in Progress - The system shall provide the ability of randomly monitoring live Video and record and review with a rewind function. Describe this feature and whether it is currently available.

✓ Securus has read, understands, and complies.

Securus Video Visitation allows real time viewing (monitoring) of video sessions and interrupt from a computer (smart phone and tablet coming soon) for authorized users. Live viewing can be done at the facility or remotely. Authorized users can view live sessions with a standard computer and a broadband internet connection.

Monitoring Video Visitation Sessions with Securus Video Visitation

Proprietary and Confidential

The screenshot displays the Securus Video Visitation dashboard. At the top, there is a header with the Securus logo and a welcome message. Below the header, the dashboard is organized into several sections: Appointments, Communications, Administration, and Commissary. The Appointments section includes links for New appointment, New appointment for others, New public appointment, and Reports. The Communications section includes Chat and Messages. The Administration section includes Users, Terminals, Locations, and Logs. The Commissary section includes Products, Product Families, and Orders. A callout box points to the 'Session Viewer' link in the Administration section, stating: 'Facility staff easily monitor visitation sessions through the Securus Video Visitation Dashboard.' Below the callout, the 'Session Viewer' table is visible, showing a list of sessions with columns for Session, Appointment, User list, Date, Start, End, Duration, and Actions.

Session	Appointment	User list	Date	Start	End	Duration	Actions
375	638	Joe Thefourth JD Ksinsky	2012-06-06	16:53:02	16:53:55	00:00:54	[Play] [Lock] [Close]
385	651	Jim Skatberg Ray Jay	2012-06-11	07:42:10	08:00:19	00:18:09	[Play] [Lock] [Close]

28 total results

The system has the capacity to simultaneously record the visitation sessions from all installed stations.

Securus Video Visitation allows the facility to record sessions either predetermined by user profile, for example all offenders, or ad-hoc, for example where suspicious behavior is seen. All recorded sessions are stored in an encrypted file format and only users with proper permissions can view recordings. Recordings are hosted in through the centralized network. All recordings are logged and time-stamped for traceability and to ensure integrity of the recordings. Securus anticipates enhancements to the recording functionality, which will include additional search capabilities, download capabilities, and recording user management capabilities.

Depending on the facility's data retention policy, Securus can set the recorder software to have 30, 60, or 90-plus day retention cycles. Transferring recordings to mobile media is available, and Securus can provide recordings on request. Administrator access to transfer recordings is currently under development.

THREADS™

A Securus exclusive, lead generating, analytic technology and is not available from any other provider. THREADS is a powerful, accurate, and extremely easy to use software application that will automatically generate leads for investigators by uncovering calling patterns, associations between multiple offenders, and their correlation to called parties.

THREADS will automatically analyze investigative data such as offender communication records, public phone records, and data from confiscated cell phones to generate focused leads for investigators. Leads can include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple offenders, their correlation to called parties, and much more.

- 4.3.2 Ability to Automatically Notify an Investigator - The system shall provide the ability to remotely notify an investigator when a targeted inmate is visiting or has visited or an IP address is being used or has been used. Describe the process.

✓ **Securus has read, understands, and partially complies.**

This function is currently on the SVV road map and targeted for development at a later time.

- 4.3.3 Transcribing Email (English and Spanish) Search - Ability to translate multiple languages from Inmate Email. Describe this feature and whether it is currently available.

✓ **Securus has read, understands, and complies.**

Securus inmate email application, Secure Instant Mail (SIM) is the application we propose for inmate email. SIM has the capability to translate between Spanish and English and English to Spanish.

- 4.3.4 Any Other Additional Investigative Tools, Features, or Creative Solutions - Describe any other tools, features, or creative solutions that might be available to MCSO.

✓ **Securus has read, understands, and complies.**

Securus' R&D staff actively works to meet the emerging and evolving needs of our customers as the use of this technology matures. We seek input from our customers to learn the market-driven needs that will help craft the future of video visitation. As an important Securus customer, when Maricopa County identifies a new, high-demand need for the system, you most likely will see it in a future release.

As we look to the future of video visitation, Securus has evaluated such uses as paid secure Internet browsing, paid games, law library access, and music/MP3 sales using the Securus Video Visitation terminals.

THREADS, a Securus exclusive, lead-generating, analytic technology, is not available from any other provider but easily could be implemented for Maricopa County's benefit. THREADS is a powerful, accurate, and extremely easy to use software application that will automatically generate leads for investigators by uncovering calling patterns, associations between multiple offenders, and their correlation to called parties.

THREADS will automatically analyze investigative data such as offender communication records, public phone records, and data from confiscated cell phones to generate focused leads for investigators. Leads can include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple offenders, their correlation to called parties, and much more.

4.4 INSTALLATION REQUIREMENTS:

- 4.4.1 All costs Associated - The contractor shall be responsible for all costs associated with the Web-based Video Visitation/Communication Kiosk System, including purchase, installation, service, maintenance and operation. The Sheriffs Office shall have no responsibility for any costs associated with the installation or on-going maintenance of the system, excluding the network.

✓ Securus has read, understands, and complies.

Securus will be responsible for all costs associated with the purchase, installation, service, maintenance, and operation of the Web-based Video Visitation/Communication Kiosk System, SVV.

- 4.4.2 Space Requirements - Please provide a of list space, environmental, and electrical power requirements.

✓ Securus has read, understands, and complies.

SVV requires the following space, environmental, and electrical power requirements:

- Space: Outside dimensions of SVV terminals are 21" x 17" x 6" (H x W x D). The video visitation application and data reside on a server that is hosted on Securus' network. This server manages all the interactions between the video visitation terminals and clients and provides secure storage of all data.
- Environmental: SVV units are designed for a typical correctional environment and do not require any special environmental conditions.
- Electrical: SVV units use a three-prong 120-volt (standard PC) power cable.

- 4.4.3 Implementation Plan - The contractor shall submit a preliminary implementation plan which shall include an installation schedule. Refer to specific requirements for expected duration of each phase. Any initial installations must be completed by the agreed upon date(s) by both parties after the contract begin date.

✓ **Securus has read, understands, and complies.**

Please refer to Appendix A: Preliminary Implementation Schedule for Securus plan, which fulfills the requirements of the RFP.

- 4.4.4 Coordinating Removal of the Current Video Visitation Systems - MCSO currently owns the Inmate Video Visitation System in place at 4th Ave Jail, Lower Buckeye Jail, and Tents Jail. When a new contractor is selected as a result of this RFP, a coordination team shall be formed for a smooth and orderly transition from the current system to the new system. This team will consist of MCSO personnel, FMD and the new contractor. This transition should cause minimum service interruptions. A new contractor may install new cable or acquire legal rights to the existing cable. Minimal disruption of service is required for new installation.

✓ **Securus has read, understands, and complies.**

Securus will complete the installation of the video visitation system and related equipment during hours specified by MCSO; Securus can install the system during "off hours" (hours when the system will not be in use by inmates, friends and family, and others) or during normal business hours. With our experience of installing video and telephone systems in our approximately 2,200 customer locations, Securus understands the importance of transitioning service with minimal disruption to facility staff and inmates.

4.4.5 System Testing

- 4.4.5.1 The Contractor must describe, in its response, how it performs standard system testing to ensure that the proposed Web-based Video Visitation/Communication System and its network services are fully implemented and ready to accept visitation traffic and MCSO use. This description must include the Contractor and industry standard methodologies, procedures and protocols consistent with the Web-based Video Visitation/Communication Kiosk System proposed for MCSO.

✓ **Securus has read, understands, and complies.**

Our Project Managers will work with Maricopa County to coordinate equipment deliveries and facility access. When the Securus Technicians arrive onsite, they may require escorts to the equipment locations. Though the majority of our project activity will occur during normal business hours, Securus can accommodate late-night/overnight cut-over activities should Maricopa County prefer.

After each facility is transitioned, our Project Manager and Field Service Technician will review our quality checklists with the Maricopa County Team.

Weekly stakeholder meetings will be hosted by the Securus Project Team and will involve participation from the Maricopa County Team.

At the beginning of the implementation project, the Securus Project Management Team will work with the Maricopa County Team to identify key stakeholders, primary points of contacts, and roles/responsibilities for the duration of the project.

The Securus Project Management Team will establish regular meeting forums and communication protocols that accommodate the requirements of the Maricopa County Team.

Throughout the duration of the project, our Project Management Team will provide weekly installation progress reports. The reports will include updates on all active, completed, and pending installation activities.

In addition to the personal communication from our Project Managers, Securus can set-up automated email notifications for the Maricopa County Team. The automated email notifications are a great way for our customers to receive updates on status changes for major milestones and other tasks of interests.

Please refer to "Appendix B: Securus Test and Acceptance Documents and Checklists."

4.4.5.2 The Contractor must describe what is required of MCSO personnel during this system testing. All hardware, software, software licensing, etc. required to perform this testing must be provided to MCSO at no cost.

✓ **Securus has read, understands, and complies.**

Securus' demand on MCSO personnel's time is minimal, requiring only the following:

- Escorts in appropriate areas for security purposes
- Project management resources and time to finalize and approve installation plans
- Project management resources and time approve work at key milestones
- Project management resources and time for final approval of system installation
- Project management resources and time for status meetings at regular intervals during installation

Securus will provide all hardware, software, software licensing, etc. to MCSO at no cost.

Please refer to Appendix A for Securus' Preliminary Project Plan.

- 4.4.5.3 The Contractor is required to provide system testing which simulates normal operating conditions of the installed Hosted Video Visitation Solution to ensure proper performance after hardware and software configuration is complete. This simulation must include full traffic load representing high traffic situations for visitation traffic.

✓ **Securus has read, understands, and complies.**

Securus goal in serving our customers is to provide the highest quality, most durable systems in the corrections industry. We strive to accomplish this in several ways, including thoroughly testing our systems under both predicted "normal" conditions as well as under full loads. During installation, we will work closely with MCSO project managers, giving regular status updates and sharing installation progress, so you will always be fully aware of the progress being made in the installation.

Please refer to Appendix B for Securus' Testing Approval form.

- 4.4.5.4 The Contractor must agree, in its response, to MCSO's right to require the replacement of any network service or system component whose failure to meet required performance levels during testing has risen to chronic problem level.

✓ **Securus has read, understands, and complies.**

Because your satisfaction and the highest-quality installation are of prime importance to us, Securus will replace any network service or system component whose failure to meet required performance levels during testing has risen to chronic problem level. We understand that faulty or non-working components costs MCSO commission revenues and deprives inmates from meeting with their friends and family as well as others.

Please refer to Appendix B for Securus' Customer Acceptance Checklist form

- 4.4.5.5 Contractor - After cutover of any portion of the system, the contractor shall conduct acceptance tests consistent with factory system performance specifications.

✓ **Securus has read, understands, and complies.**

Because your satisfaction and the highest-quality installation are of prime importance to us, Securus shall conduct acceptance tests consistent with factory system performance specifications to ensure the proper operation of the system.

Please refer to Appendix B for Securus' Customer Acceptance Checklist form

4.4.5.6 MCSO - The Sheriff's Office shall also complete a test regimen based upon features and performance as specified in the contract.

✓ **Securus has read, understands, and complies.**

Securus will work with and cooperate in every way so that the Sheriff's Office can complete a test regimen based upon features and performance as specified in the contract.

4.4.5.7 Action Item List - An action item list will be developed for any issues resulting from the testing. A mutually agreed upon time table will be developed and implemented for all action items to be resolved.

✓ **Securus has read, understands, and complies.**

In meeting regularly with MCSO Project Managers, we will work together to identify all action items for any issues resulting from the testing and develop mutually agreed upon time table to resolve the items.

4.5 MAINTENANCE, SERVICE AND SUPPORT:

4.5.1 The contractor must submit a detailed explanation of the maintenance and repair plan. If the problem involved is an equipment failure, MCSO shall be provided a root cause analysis report within thirty (30) days of the incident.

✓ **Securus has read, understands, and complies.**

Securus SVV is centrally monitored and managed through the most comprehensive maintenance and repair network in the corrections industry. Monitoring begins with our state-of-the-art Network Operations Center (NOC), extends to our Technical Support Center, and on-site maintenance will be handled by the on-site administrators assigned to MCSO supplemented by field services technicians strategically located to provide any additional support needed.

SVV is constantly monitored by Securus employees from our NOC at our headquarters location in the metropolitan Dallas, Texas, area. This service center is staffed 24x7x365 by network experts who are certified in the systems and software used to monitor all SCP functions and equipment, as well as the associated network. The NOC maintains failure reports, service history, and other diagnostic information, which will be available to the County when requested.

The NOC will maintain the names and contact information for each Securus employee supporting Maricopa County. They will be accountable for any actions required to prevent or repair any outages. Securus will follow the County's protocols for communicating outages or repair actions in the unlikely event these occur.

Securus Network Operations Center in Dallas, TX



Premium Network Monitoring Capabilities

Securus proactively identifies potential system and network abnormalities through a centralized diagnostic application, Orion by Solar Winds. This network management software allows Securus personnel to continuously monitor all hardware, software, and system metrics.

Through our network monitoring practices, we are able to complete the following functions:

- **Enable proactive repairs to a system to prevent it from going down.** Many times corrections are made before a system shows signs of an issue and before the facility is aware of a problem. This means less down time and increased system reliability for the facility.
- **Alert remote or on-site engineers of any system threshold inconsistencies or alarms.**
If detected:
 - Alerts are sent to the NOC to track the event.
 - The NOC communicates with engineers through email, short message service (SMS), or directly through a wireless phone to address the issue.
- **Receive real time alerts when the system detects an error.**
 - Identifies if the network elements health threshold has been exceeded or if any other potential system issue has been discovered.

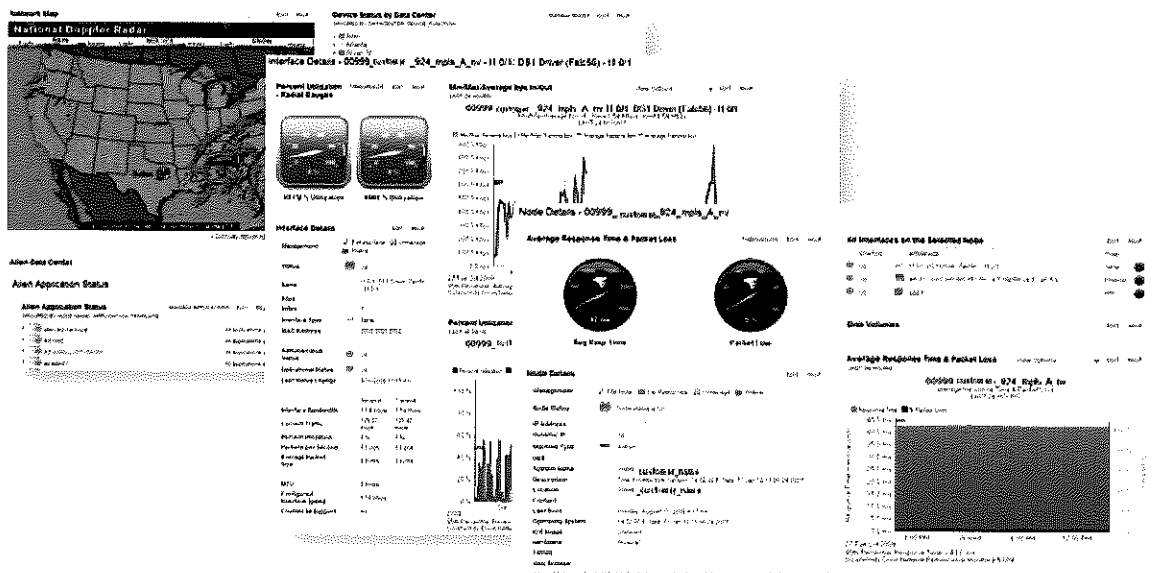
- Establishes volume thresholds for each transport carrier on core node equipment at each data center, alerting Securus personnel of possible carrier network issues.
- **Monitor call traffic patterns, bandwidth detail, and network life cycle management to ensure sufficient resources are in place.** A separate capacity engineering team reviews call traffic volume reports and storage requirements throughout all systems.
- **Centrally monitor all calling traffic and reporting to determine if increase or decreases in the number of telephones are needed.** Upon agreement by the County, the service and operations team will install any additional telephones required.

Remote Programming, Diagnostics, and Troubleshooting

The Securus NOC uses the Orion network monitoring application to constantly check the system to ensure optimum performance and to anticipate the need for additional network or capacity.

Visual monitoring in our NOC is achieved through the use of several key screens that are constantly updated and monitored by our personnel in our NOC.

Sample Network Operations Center Monitoring Screens



The NOC can contact the Technical Support Center (TSC) if it determines that another level of technical support may be needed to address issues or concerns. This action could involve dispatching a Field Services Technician to a Maricopa County facility.

A description of our next team, the Technical Support Center, follows and continues to demonstrate the importance of our integrated teams.

Technical Service Center

Securus is the only corrections industry provider that has made a strategic decision to centralize management of all technical services support. We provide superior customer service capabilities from a state-of-the-art technical service support center located in the metropolitan Dallas, Texas, area at 3000 Kellway Drive Suite 150; Carrollton, Texas 75006.

The Securus Technical Services Center (TSC) is staffed by approximately 50 technical center professionals and handles approximately 8,000 inbound queries per month. The TSC uses a call distribution system to automatically manage the flow of inbound customer calls. The TSC provides a single-point-of-contact where a facility may inquire on items such as remedial maintenance issue or trouble that may arise 24x7x365. Clients can contact the TSC by any of the following convenient methods to obtain service:

- **Telephone** – 866-558-2323
- **E-Mail** – technicalsupport@securustech.net
- **Fax** – 800-368-3168
- **Web portal** - <http://www.securustech.net/facility/Default.asp>

The technical service center offers the following features to our clients:

- Technical support and field dispatch 24x7x365
- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure Service Level Agreements are met
- Certified technicians to provide quick problem resolution
- Ownership of every issue via training, support, other departments, and historical information
- System and individual site connectivity monitored 24x7x365

24x7x365 Securus Technical Support Center



Securus technicians receive internal Securus certifications, based on our business and the products and services we support.

Service Levels

When a facility calls Securus, the event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a resolution timeline and escalation procedure. In all cases, Technical Support will respond in the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when a system event adversely affects the operations in multiple housing units.

Response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides an estimated time of arrival.

A P1 event is escalated to the following groups and persons:

- Technical Support Department

- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Priority 2 Service Level

A Priority 2 (P2) assignment occurs when a system event adversely affects system functionality ion and entire housing unit.

Response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides and estimated time of arrival. A P2 event is escalated to the Technical Support Department.

Priority 3 Service Level

A Priority 3 (P3) assignment occurs when a system event adversely affects a single terminal or multiple terminals.

Response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides and estimated time of arrival. A P3 event is escalated to the Technical Support Department.

Escalations

If a dispatch is not required, Securus notifies the facility when the service issue is resolved. If a technician is required, Securus contacts the customer with an estimated time of arrival.

The following supervisory personnel represent the escalation chain:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- VP Service and Technical Operations

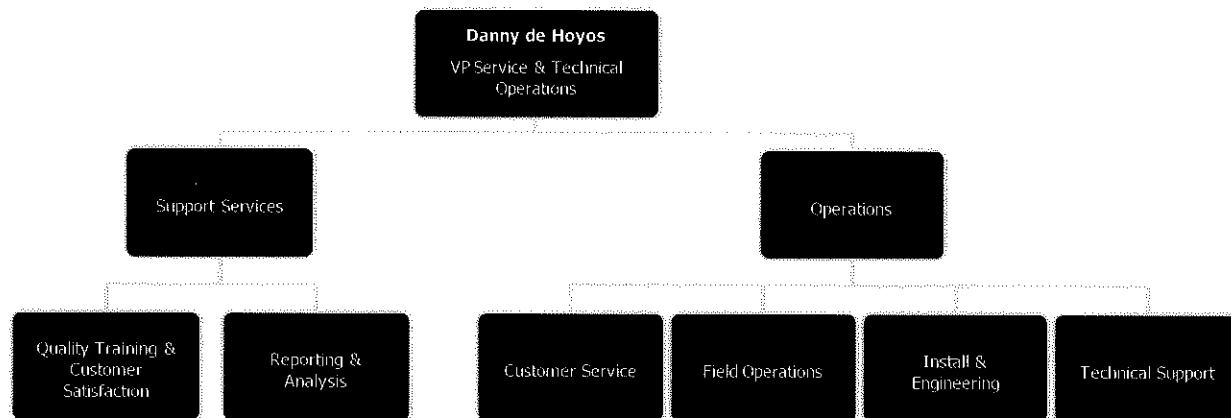
Centralized Services Operations Model

All Securus' services and operations are managed centrally, from our Services and Operations organization in the metro-Dallas, Texas area. The Operations team is responsible for supporting external customers; this includes Customer Service, Field Services, Installation and Engineering,

and Technical Support. The Support Services team is responsible for providing internal support services; this includes Quality, Training and Customer Satisfaction, and Reporting and Analysis.

The following figure diagrams the Securus Services and Operations organization, which staffed by dedicated full-time Securus employees.

Services and Operations Organization



One of the main reasons for adopting this operational model was the natural interaction between each functional group. Having our support services integrated and centrally managed enables cross-functional group interaction, which improves the response, resolution, and efficiencies of our services.

Also important to note, for service organizations that provide local customer support, such as Field Services, our centralized services operational model enhances the local support we provide to our customers and improves our overall response. For example, the centralized services operations model enables tight integration between the Technical Support and the dispatch team within Field Services, facilitating a coordinated effort that improves our local, field related support—including installations, upgrades, maintenance, and equipment repairs for Securus supported solutions.

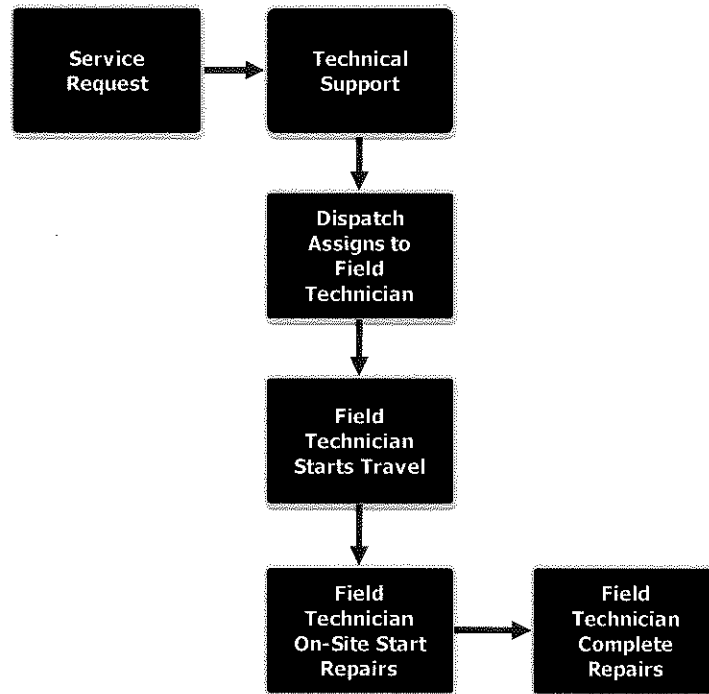
Service Ticket Routing

The TSC manages the flow of inbound calls through a call distribution system that routes calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our key objective of providing timely resolution to each request. Service calls are answered 24x7x365 by live technicians to provide timely and quality customer service.

Field Service Technicians (FSTs) will be routed to all service requests through the Securus trouble ticketing process. The Securus trouble ticket process is illustrated in the following figure.

Trouble Ticketing Process

Proprietary and Confidential



In all instances, service will be requested through the TSC and service personnel will be dispatched through trouble ticketing system to ensure documentation and timely resolution of all service tickets.

Event Tracking System

The Securus event tracking system logs, tracks, manages, and assures appropriate response to all service requests. The service request generates a unique trouble ticket number that is linked to each facility's service history and provides real-time updates. Each ticket has a priority level assignment, which drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem, and resolves the problem or engages the appropriate party for problem resolution.

The TSC maintains ownership of all service requests and is responsible for the escalation and update functions. Every effort is made to resolve problems remotely and within the framework of resolution timeframes. However, if the problem requires on-site service, a technician will be dispatched to the facility to expedite resolution. Securus will contact the facility to arrange for the on-site service at the convenience of the facility.

County facilities can also open and track trouble tickets through our convenient facility portal.

Facility Portal

Securus provides partnering facilities like Maricopa County with one of the only web-based, anywhere, anytime single-point access customer portals in the industry. At any time, day or night, 24x7x365, Maricopa County can securely access details about your facility's operations. Approved users can access all calling activity, including all call detail reports.

The Facility Portal can serve as the user interface to Securus' electronic trouble ticket system and allows authorized users to perform functions such as creating and managing service tickets and generating reports. With Facility Portal, users can initiate trouble tickets for repairs, track the real-time status, and generate current and historical reports of these tickets. After a ticket is generated, a tracking number is automatically and immediately created. All updates are sent in real-time electronically to the originator of the ticket, as well as to the County designee.



Facility Portal Service Center

The Service Center will allow the user to create and manage their facility's technical support tickets. As needed, users can search for service tickets by entering the ticket number in the search field or by selecting date search

The following figure provides an example of the screen used to manage service tickets.

Manage Your Service Tickets

Proprietary and Confidential



FRIENDS & FAMILY CORRECTIONAL FACILITIES ABOUT US CAREERS CONTACT US

Facility Portal

Facility Name

Dashboard
Portal Manager
Commissions Reports
General Reports
Order Materials
Downloads & User Guide
Service Center
 Your Tickets
 Create A Ticket
 Date Search

Search Tickets

Help
Secure Call Platform
Log-Out

Your Service Tickets

SITE NAME	TICKET #	DESCRIPTION	LAST UPDATED	STATUS
Facility Name	13802698	Div 11 VB enrollments	2011-08-16 09:56:04	Closed
Facility Name	13799289	Voice Biometrics - the customer is enrolling/re-enrolling inmates in VB at Division 11...	2011-08-12 11:06:18	Closed
Facility Name	13792501	Report Request: Calls completed in 2008 from Division 1, Tier 8-4 Call period is 9/1...	2011-08-05 15:19:43	Closed
Facility Name	13783054	customer reports that he creates an iso image to burn to DVD and when image was downlo...	2011-07-29 10:24:54	Closed
Facility Name	13782536	Voice Biometric - Re-enrollments the customer is doing re-enrollments of inmates at t...	2011-07-28 11:10:58	Closed

1 2 3 4
Total Tickets

By clicking on the ticket number, a detailed report pops up. If a ticket is closed, you can review all the previous notes and the final resolution at any time. If the ticket is currently open, you can create a new journal note. Consent to close a ticket can also be performed using the notes section.

The following figure provides an example of ticket detail.

Ticket Detail

Proprietary and Confidential

The screenshot displays the Securix Facility Portal interface. At the top, the Securix logo is visible with the tagline "Supporting what matters". Below the logo is a navigation bar with links: "FRIENDS & FAMILY", "CORPORATE FACILITIES", "ABOUT US", "CAREERS", and "CONTACT US". The main heading "Facility Portal" is prominently displayed. On the left side, there is a sidebar menu with the following items: "Marketing", "Dashboard", "Portal Manager", "Reports", "Order Materials", "Downloads & User Guide", "Service Center", "Your Tickets", "Create A Ticket", "Data Search", "Search Tickets", "Help", and "Logout". The main content area is titled "Ticket Details #13529104". It shows a "Ticket ID: 13529104" and a "Can Description: Terrace and indoor phone not working". Other details include "Ticket Priority: 3", "Ticket Status: Closed", "Date Opened: 12/29/2019 8:14:24 AM", and "Last Update: 12/29/2019 8:51:24 AM". The "Solution Description" is "reset signal". Below this, a table lists "Associated Work Orders":

Work Order ID	Work Order Description	Work Order Status
13529104	12/29/2019 8:14:24 AM	Active Requested - Waiting for Customer Approval
13529104	12/29/2019 8:51:24 AM	Assignment Completed from Manager

At the bottom of the ticket details, there is a link to "View A New Journal Entry".

Create a Service Ticket

To open a service ticket, select create a ticket and then complete the service ticket form. The following figure provides an example of the screen used to open service tickets.

Open Service Ticket

Proprietary and Confidential



FRIENDS & FAMILY CORRECTIONAL FACILITIES ABOUT US CAREERS CONTACT US

Facility Portal

Facility Name

Create Service Ticket

Dashboard
Portal Manager
Commissions Reports
General Reports
Order Materials
Downloads & User Guide
Service Center
Your Tickets
Create A Ticket
Data Search
Search Tickets

Site:

Facility Name

Problem Category:

Please Choose a Category

Suggested Priority:

Please Choose a Category

Problem Description:

CDR Report Question/Request
Full Outage
Inmate Can't Place Call
Other
Partial Outage
Password Reset
Phone/Equipment Replacement
PIN Reset
SCP User Interface Question

Submit Ticket

For the Field Services organization, operations are tightly integrated between Securus' Technical Support organization and the dispatch team within Field Services, facilitating a coordinated effort that improves our local, field related support, including installations, upgrades, maintenance, and equipment repairs for Securus supported solutions.

Our services operational model is designed to take advantage of the natural interaction between the technical support and field services teams. Having our support services integrated and centrally managed enables cross-functional group interaction, which improves the response, resolution, and efficiencies of our services.

The Securus Field Services Team

The Securus Field Services organization employs one of the largest bases of in-house field service support personnel in the inmate phone system industry. Our team consists of approximately 150 Field Service Technicians (FST) located throughout the United States, which includes a team of FSTs with the requisite knowledge to support the systems in Wisconsin. As required, our resident teams expand based on our growing customer needs.

Our field services team installs and maintains inmate phone systems for approximately 2,200 facilities and approximately 850,000 inmates in 45 states. The Securus Field Operations Director is supported by three regional Service Managers who possess more than 60 years of combined field service experience, lead the Securus field service team.

Each member of our Field Services team receives on-the-job training and the equipment certifications required to install and maintain the equipment in the customer's facility. Additionally, each FST is equipped with the latest tools and equipment, including company provided laptops, cell phones, vehicles, and spare parts to expedite repairs and minimize system downtime.

Each FST will be capable of completing a security screening prior to admittance to your facility. All field services support is provided to the counties in Wisconsin and throughout the United States by the Securus team at no charge.

Field Service Technician Standards

Securus' Field Services organization requires that all Field Services Technician (FST) personnel meet the following standards:

- **Are strategically located throughout the U.S.**– Our FSTs are located throughout the United States in strategic geographic locations that enable them to meet our clients' response time needs.
- **Meet educational and certification standards** – All FSTs are thoroughly screened before employment, and are required to have an extensive telecommunications background. Additionally, FSTs receive extensive Securus' training and certifications to support our product offerings.
- **Receive product and engineering support** – Our in-house integrated support model keeps our technical support team engaged throughout problem resolution. FSTs and the technical support team have direct access to product and development engineers, enabling them to expedite repairs and minimize customer downtime.
- **Carry standard tools and parts** – All FSTs carry a complete set of tools and standard truck stock of parts to handle the majority of repair requests; these include telephone sets, handsets, dials, and replacement circuit boards, which they keep in their truck or on-site. If a technician does not have the spare part in his or her truck or at the site, Securus will drop-ship the item to the site; or if the situation is critical, Securus will ship counter-to-counter parts orders from our central warehouse on the same day.

Our certified technicians are able to respond to critical issues within four hours or less if required by specific County requirements. These technicians also have immediate access to engineering resources should there be a need. The technician is required to follow a structured technical and management escalation process if they are unable to isolate the problem within four hours.

Field Service Manager

- Conduct remote visits via phone bimonthly. Based on information obtained from call, a trouble ticket may be opened

- Work with the account team to evaluate contract progress with the County quarterly
- Provide the facility with applicable site information that assists them based on the account profile.
- Monitor ticket traffic
- Resolve escalation issues, as needed

Each field service manager possesses the skills required to perform the duties of the field technician and can provide additional or backup support as needed.

- 4.5.2 The Contractor must provide all post installation system programming and maintenance services at no cost to MCSO

✓ **Securus has read, understands, and complies.**

All post installation system programming and maintenance services will be provided at no cost to MCSO.

- 4.5.3 The Contractor must warrant that the Web-based Video Visitation/Communication Kiosk System installed for the MCSO facilities shall be free of defects, irregularities, unprofessional installation, code violations and shall operate as designed and proposed. Should the system not operate as designed and proposed or violate any local, state or federal code, the Contractor shall immediately correct the defect or irregularity or bring the system within code and performance specifications at no cost to MCSO.

✓ **Securus has read, understands, and complies.**

Securus warrants that SVV will be free of defects, irregularities, unprofessional installation, and code violations and shall operate as designed and proposed. Securus will immediately correct the system should it not operate as designed and proposed or violate any local, state or federal code.

- 4.5.4 Should any critical component of the Web-based Video Visitation/Communication Kiosk System provided by the Contractor fail, the Contractor must respond to Web-based Video Visitation/Communication Kiosk System maintenance/repair calls from MCSO in the manner outlined in this section.

✓ **Securus has read, understands, and complies.**

- 4.5.5 Service Priority Levels - Trouble Tickets:

4.5.5.1 Priority Level One - A priority level one service issue occurs when the entire system fails, a jail system fails, or multiple housing units are not operational. A technician shall be on site and the repairs shall occur within 2 hours.

✓ **Securus has read, understands, and complies.**

When a facility calls Securus, the event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a resolution timeline and escalation procedure. In all cases, Technical Support will respond in the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when an entire system fails or multiple housing units are not operational.

Response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides an estimated time of arrival.

A P1 event is escalated to the following groups and persons:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

4.5.5.2 Priority Level Two - A priority level two service issue occurs when one entire housing unit is not operational. Repairs shall occur within 24 hours maximum.

✓ **Securus has read, understands, and complies.**

A Priority 2 (P2) assignment occurs when a system event adversely affects system functionality in an entire housing unit.

Response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides an estimated time of arrival. A P2 event is escalated to the Technical Support Department.

- 4.5.5.3 Priority Level Three - A priority level three service issue occurs when one or more kiosks in a housing unit are not operational. Repairs shall occur by the end of the next business day.

✓ **Securus has read, understands, and complies.**

A Priority 3 (P3) assignment occurs when a system event adversely affects a single terminal or multiple terminals.

Response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides an estimated time of arrival. A P3 event is escalated to the Technical Support Department.

Securus can meet this requirement through the on-site technicians that will be assigned to Maricopa County Jail.

- 4.5.6 Reporting Repair Problems - Describe the method of reporting repair problems. State whether or not MCSO will have access to the reports.

✓ **Securus has read, understands, and complies.**

Maricopa County will use Securus' exclusive, convenient, user-friendly Facility Portal to gain insight into commission information, to open and track trouble tickets, and to order marketing materials related to SVV. The Securus-provided on-site technicians will also support the facility by opening and tracking any service tickets through the Facility Portal. Although authorized personnel can generate reports themselves, the site administrators also will assist with any reports if needed by Maricopa County personnel.

Facility Portal

Securus provides partnering facilities with one of the only anywhere, anytime single-point access customer portals in the industry. At any time, day or night, 24x7x365, Maricopa County can use our SCP user interface to securely access the facility's operations. Approved users can access all calling activity, including all call detail reports.



The Facility Portal can serve as the user interface to Securus' electronic trouble ticket system and allows authorized users to perform functions such as creating and managing service tickets and generating reports. With Facility Portal, users can initiate trouble tickets for repairs, track the real-time status, and generate current and historical reports of these tickets. After a ticket is generated, a tracking number is automatically and immediately created. All updates are sent in real-time electronically to the originator of the ticket, as well as to the County designee.

Facility Portal Service Center

The Service Center will allow the user to create and manage their facility's technical support tickets. As needed, users can search for service tickets by entering the ticket number in the search field or by selecting date search

The following figure provides an example of the screen used to manage service tickets.

Manage Your Service Tickets
Proprietary and Confidential

SECURIX
connecting what matters™

FRIENDS & FAMILY **CORRECTIONAL FACILITIES** ABOUT US CAREERS CONTACT US

Facility Portal

Facility Name

Dashboard
Portal Manager
Commissions Reports
General Reports
Order Materials
Downloads & User Guide
Service Center
Your Tickets
Create A Ticket
Date Search
Search Tickets
Help
Secure Call Platform
Log-Out

Your Service Tickets

SITE NAME	TICKET #	DESCRIPTION	LAST UPDATED	STATUS
Facility Name	13802698	Div 11 VB enrollments	2011-08-16 09:56:04	Closed
Facility Name	13799289	Voice Biometrics - the customer is enrolling/re-enrolling inmates in VB at Division 11...	2011-08-12 11:06:18	Closed
Facility Name	13792501	Report Request: Calls completed in 2008 from Division 1, Tier B-4 Call period is 9/1...	2011-08-05 15:19:43	Closed
Facility Name	13783054	customer reports that he creates an iso image to burn to DVD and when image was downlo...	2011-07-29 10:24:54	Closed
Facility Name	13782536	Voice Biometric - Re-enrollments the customer is doing re-enrollments of inmates at t...	2011-07-28 11:10:58	Closed

1234
Total Tickets

By clicking on the ticket number, a detailed report pops up. If a ticket is closed, you can review all the previous notes and the final resolution at any time. If the ticket is currently open, you can create a new journal note. Consent to close a ticket can also be performed using the notes section.

The following figure provides an example of ticket detail.

Ticket Detail

Proprietary and Confidential

The screenshot displays the Securix Facility Portal interface. At the top, the Securix logo is visible with the tagline "Securing what matters". Below the logo is a navigation bar with links: FRIENDS & FAMILY, COMMERCIAL FACILITIES, ABOUT US, CAREERS, and CONTACT US. The main heading "Facility Portal" is prominently displayed. On the left side, there is a sidebar menu with options: Marketing, Dashboard, Portal Manager, Reports, Order History, Downloads & User Guide, Service Center, Open Tickets, Create A Ticket, Date Search, Search Tickets, > Open, and Logout. The main content area is titled "Ticket Details #13529104". It shows the following information: Call Description: Service and Network outage not working, Ticket Priority: 3, Ticket Status: Closed, Date Opened: 12/28/2010 8:14:24 AM, Last Update: 12/28/2010 8:51:24 AM, and Solution Description: reset sigs. Below this, there is a section titled "JOURNAL NOTE ENTRIES" containing a table with two entries. The first entry has a timestamp of 12/28/2010 8:40:21 AM and the text "Issue Resolved - Waiting for Customer Approval". The second entry has a timestamp of 12/28/2010 8:50:17 AM and the text "Assignment Completed from Manager". At the bottom of the ticket details section, there is a link that says "Create A New Journal Entry".

Create a Service Ticket

To open a service ticket, select create a ticket and then complete the service ticket form. The following figure provides an example of the screen used to open service tickets.

Open Service Ticket

Proprietary and Confidential

SECURUS
TELEVISION & VIDEO
connecting what matters™

TEEN & FAMILY CORRECTIONAL FACILITIES ABOUT US CAREERS CONTACT US

Facility Portal

Create Service Ticket

Facility Name

Site: Facility Name

Problem Category: Please Choose a Category

Suggested Priority: Please Choose a Category

Problem Description:

- CDR Report Question/Request
- Full Outage
- Inmate Can't Place Call
- Other
- Partial Outage
- Password Reset
- Phone/Equipment Replacement
- PIN Reset
- SCP User Interface Question

Submit Ticket

Dashboard

Portal Manager

Commissions Reports

General Reports

Order Materials

Downloads & User Guide

Service Center

Your Tickets

Create A Ticket

Data Search

Search Tickets

- 4.5.7 Escalation List - Within 10 days of award of contract, provide a list of contact names, telephone numbers, and e-mail addresses for escalation of unresolved service requests and issues that are not resolved.

✓ **Securus has read, understands, and complies.**

Within 10 days of being awarded the contract for Maricopa County's VVS services, Securus will provide the names, telephone numbers, and email addresses for escalation of unresolved service requests.

- 4.5.8 Service Availability - The contractor shall be available to service equipment and the Web-based Video Visitation/Communication Kiosk System when a priority level one or two service issue occurs 365 days per year without additional cost to MCSO. Priority level three services will be completed during regularly scheduled work hours, Monday through Friday.

✓ **Securus has read, understands, and complies.**

Securus is built on providing responsive customer service. Because your facility is open and operating 24x7, so are we. We monitor the network your VVS will run on 24x7 and have service personnel always at the ready to meet any service need that may arise. We will have on-site technicians or field service associates prepared to respond to priority level one and two service issues with the two and 24-hour requirements, respectively.

- 4.5.9 System Checks - The contractor will perform system checks and preventative maintenance on a monthly basis to ensure the system is operating at optimum efficiency and performance. A system check and preventative maintenance logbook, that includes the findings and specified action, will be maintained by the Contractor and remain at a MCSO specified location.

✓ **Securus has read, understands, and complies.**

Securus proactively identifies potential system and network abnormalities through a centralized diagnostic application, Orion by Solar Winds. This network management software allows Securus personnel to continuously monitor all hardware, software, and system metrics.

Through our network monitoring practices, we are able to complete the following functions:

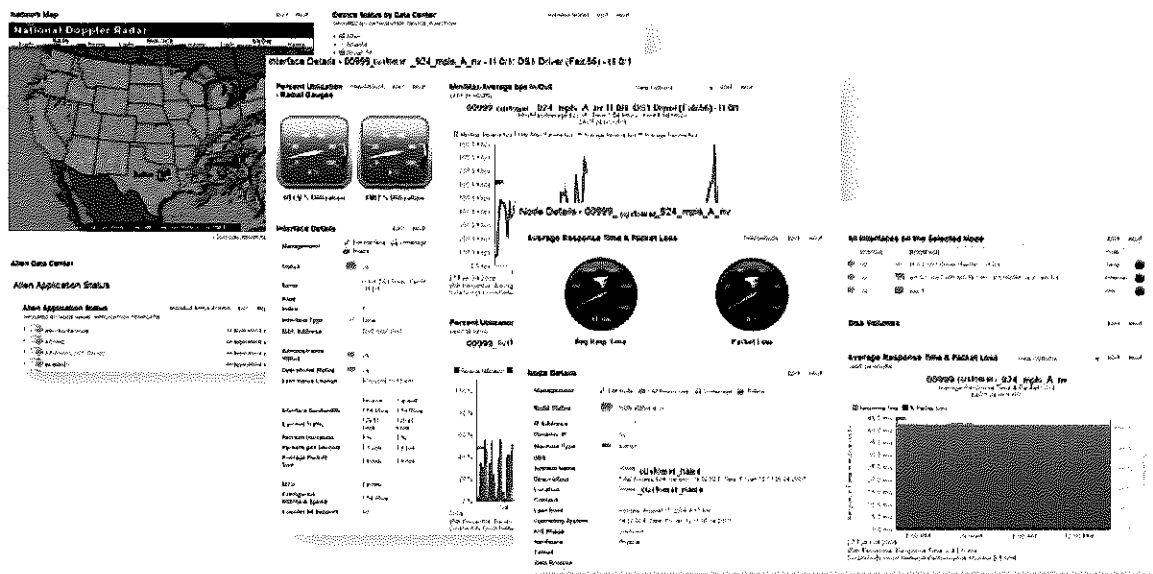
- **Enable proactive repairs to a system to prevent it from going down.** Many times corrections are made before a system shows signs of an issue and before the facility is aware of a problem. This means less down time and increased system reliability for the facility.
- **Alert remote or on-site engineers of any system threshold inconsistencies or alarms.** If detected:
 - Alerts are sent to the NOC to track the event.
 - The NOC communicates with engineers through email, short message service (SMS), or directly through a wireless phone to address the issue.
- **Receive real time alerts when the system detects an error.**
 - Identifies if the network elements health threshold has been exceeded or if any other potential system issue has been discovered.
 - Establishes volume thresholds for each transport carrier on core node equipment at each data center, alerting Securus personnel of possible carrier network issues.
- **Monitor call traffic patterns, bandwidth detail, and network life cycle management to ensure sufficient resources are in place.** A separate capacity engineering team reviews call traffic volume reports and storage requirements throughout all systems.
- **Centrally monitor all calling traffic and reporting to determine if increase or decreases in the number of telephones are needed.** Upon agreement by the County, the service and operations team will install any additional telephones required.

Remote Programming, Diagnostics, and Troubleshooting

The Securus NOC uses the Orion network monitoring application to constantly check the system to ensure optimum performance and to anticipate the need for additional network or capacity.

Visual monitoring in our NOC is achieved through the use of several key screens that are constantly updated and monitored by our personnel in our NOC.

Sample Network Operations Center Monitoring Screens



- 4.5.10 Kiosk Service Standards - Each instrument and phone enclosure shall be cleaned and wiped each time it is serviced, if needed.

✓ Securus has read, understands, and complies.

As a maintenance standard, Securus technicians clean and wipe terminals when they are services if needed.

- 4.5.11 Vandalism - Any act of vandalism or machine break-ins discovered by the Contractor shall be reported immediately to the Inmate Kiosk System Administrator, or his designee. The Contractor will be totally responsible for any loss due to acts of vandalism or other loss.

✓ **Securus has read, understands, and complies.**

Securus will be responsible for repairing any vandalized or damaged terminals and shall report such findings to the Inmate Kiosk System Administrator, or his designee.

4.5.12 The Contractor must propose a Web-based Video Visitation/Communication Kiosk System that provides for remote diagnostics and maintenance.

✓ **Securus has read, understands, and complies.**

The SVV solution is a Web-based, centralized system that allows for remote diagnostics and maintenance as well as automatic technology and feature upgrades. After the video visitation system has been implemented, it is easy for Securus to enable new features and modules by activating the feature in the centralized system.

Designed to meet the needs of the facility *as defined by the facility*, Securus Video Visitation offers both at-home and on-site solutions.

Securus proactively identifies potential system and network abnormalities through a centralized diagnostic application, Orion by Solar Winds. This network management software allows Securus personnel to continuously monitor all hardware, software, and system metrics.

4.5.13 System Failure - Please describe in detail the system's failure back up plan.

✓ **Securus has read, understands, and complies.**

Securus' system failure backup plan is derived from our recovery plan for our phone systems, which are installed in about 2,200 locations across the nation.

We will develop and maintain toll-free, 24-hour-a-day, 7-day-a-week emergency access phone number lists that will be readily available for use in any emergency situation. Contact information will be updated at regular intervals to ensure accuracy. Securus' National Service Center will also maintain these emergency contact phone number lists and coordinate on a regular basis with field staff to ensure that all lists are accurate. In addition, Securus will develop relationships with local vendors who can support emergency recovery operations with the required services, supplies, and equipment.

Technical Support

Securus understands that throughout the duration of a critical event, our customers rely on our support to guide them with minimal loss of data and equipment. Qualified resources will be available to assist Maricopa County. These resources include the approximately 150 full-time field technicians who can deploy nationwide, and a full list of contacts—up to and including Securus executives.

We also realize that during a disaster, it may be even more important that offenders and detainees can stay in contact with their friends and family. To support these end users, Securus maintains two call centers in Dallas, TX, and Atlanta, GA, that can continue session processing, even if there is a failure at one location.

Coordination

Coordination of all declared emergencies will depend on the emergency level. Field staff will coordinate the emergency response to all level 3 conditions. Headquarters will provide assistance at the request of field management for Level 2 emergency conditions and will coordinate all Level 1 emergency efforts.

The field management team will develop mutual agreements with other Securus regions in the country or with vendors to supply resources, equipment, or manpower. Additional equipment and personnel may not arrive for several days, depending on available transportation, condition of the roadways and airports, and other factors, therefore field management will not delay the decision to ask for assistance from other sources.

Mobilization

Mobilization of a Headquarters Response Team, if necessary, will depend on need, as determined by the headquarters and field management.

The Headquarters Response Team will be dispatched from Dallas as soon as possible to assist field recovery efforts. However, field staff will begin recovery operations without delay.

Emergency Response Teams

Securus will form the following teams to respond to declared emergency conditions. These teams will include subject matter experts and necessary support staff.

Table: Emergency Response Teams	
Team	Manning and Responsibility
Field Local Recovery Team	Plans and directs local recovery operations Staffed by field staff personnel only
Headquarters Support Team	Provides technical support and assistance to local recovery teams Staffed cross-functionally, as required
Headquarters Response Team	Deployed to Securus local markets to assist local recovery operations The Headquarters Response Team is staffed by subject-matter experts and led by headquarters operations management

Recovery

Recovery operations may last several hours, several days, several weeks, or longer. Field staff will continue recovery operations until critical offender calling functions have been recovered and Securus can restore phone service operations to normal call and data transmission capability. Senior Securus management will, at that time, recall the Headquarters Response Team and field staff will return to normal operation. Recovery operations may still continue but emergency operations are no longer necessary and are not cost effective to maintain.

Throughout emergency recovery operations, the headquarters and field staff record all recovery actions. Following the resolution of emergency response operations, all recovery teams and appropriate management submit pertinent information and comments to be included in the Post Mortem report.

4.6 WARRANTY:

The contractor shall provide 100% warranty for the software and hardware of the Web-based Video Visitation/Communication Kiosk System for the duration of the contract at no cost to MCSO.

✓ Securus has read, understands, and complies.

Securus warrants 100 percent of the software and hardware of the web-based Video Visitation/Communication Kiosk System for the duration of the contract at no cost to MCSO.

- 4.6.1 The Contractor is responsible for replacement of the Web-based Video Visitation/Communication Kiosk System in its entirety or its individual components regardless of cause including, but not limited to, normal wear and tear due to regular use, inmate abuse and inmate unrest, and natural or man-made disasters including cyber- attacks and/or cyber-terrorism. This system or component replacement will be performed at no cost to MCSO and will occur immediately upon notification to the Contractor of the system problem by MCSO facility. The Contractor must replace visitation kiosks requiring repair and not repair components of the visitation kiosks on site at MCSO.

✓ Securus has read, understands, and complies.

As telecommunication professionals whose sole focus is service the corrections industry with the most advanced, highest quality video visitation and telephone systems, Securus understands the importance of maintaining components in top working order and promptly repairing or replacing individual parts or entire systems for any reason, such as normal wear and tear, inmate abuse and unrest, and natural or man-made disasters including cyber- attacks and/or cyber-terrorism. Should a component or the entire system need to be replaced, Securus will do this at no cost to MCSO.

4.7 TRAINING:

- 4.7.1 Initial Training - The contractor shall provide training to familiarize all MCSO personnel with the Web-based Video Visitation/Communication Kiosk System.

An outline of your training program, including subjects, time-frames, and schedule shall be provided with your response.

✓ **Securus has read, understands, and complies.**

SVV training covers all current system features and will provide additional training as more are added and the system enhanced. Securus uses our own experienced employees to conduct all training through online instructor-led classes or on-site, one-on-one and classroom training sessions at no cost to you. Standard training includes using both hands-on experience with your data and using instructor demonstrations to ensure each trainee understands all SVV concepts.

Securus training programs enable facility staff to use all features the first day of installation. Since products are Web-based, after a two- to three- hour training session most officers find it easy to maneuver through the features immediately.

In addition to standard training, Securus will work with Maricopa County to customize your online training experience to meet the unique needs of your staff and facility. We offer separate classes focused on different agency functions such as, creative investigations, well-organized live call monitoring, and efficient system administration. Training for product upgrades, new facility staff, or a general refresher course is offered through online instructor-led courses available twice a month throughout the year—*Securus ongoing training ensures your staff always "stays on top" current and newly released SVV features.*

SVV Training Course Modules

Securus is committed to providing your staff with training that will maximize the potential of the features implemented at your facility. Training courses are in a user-friendly, task-oriented format to teach your officers what they need to know to do their job. We present courses in separate modules based on the types of duties officers tend to perform using the SCP inmate telephone system while expressing the unique features of applications.

The following table presents the standard SCP training course modules and associated learning objectives.

SVV Course Modules

Course Module	Objective
Overview and Navigation	<ul style="list-style-type: none"> • User types • Appointment types • Process flow • URL - status bar - webcam • Internet speed - storage term • Three main modules

Course Module	Objective
Appointments	<ul style="list-style-type: none"> • Stop or cancel a session • Change date/time • Change terminal • Live monitor sessions
Administration	<ul style="list-style-type: none"> • Users and user groups • Terminals and locations • Logs
Session Viewer	<ul style="list-style-type: none"> • View a recorded session • Actions and icons - search, play, lock, delete
Visitation Schedule	<ul style="list-style-type: none"> • Customized by user type
Optional Applications	<ul style="list-style-type: none"> • Sick Call - symptoms • Commissary Ordering • Automated inmate information

4.7.2 The Contractor must provide all end-user training to the MCSO at no cost.

✓ **Securus has read, understands, and complies.**

Securus provides training as part of our service to Maricopa County and does not charge for it. In addition, Securus will provide refresher training as required as well as train new MCSO personnel as needs arise.

4.7.3 The Contractor must provide all end-user training on site at the various MCSO facilities.

✓ **Securus has read, understands, and complies.**

Securus will provide all training at the various MCSO facilities.

4.7.4 The Contractor must provide training for various levels of MCSO personnel including full-time system administrators, part-time system administrators, special investigators, and data entry specialists, etc.

✓ **Securus has read, understands, and complies.**

Securus will train all personnel identified by Maricopa County.

- 4.7.5 The Contractor must provide full training for all assigned system users on how to create, delete and modify inmate programming and profiles.

✓ **Securus has read, understands, and complies.**

Authorized users will be trained in all system functions, including how to create, delete and modify inmate programming and profiles.

- 4.7.6 The Contractor must provide full training for all assigned system users on how to generate appropriate system reports.

✓ **Securus has read, understands, and complies.**

Authorized users will be trained in all system functions, including how to generate appropriate system reports.

- 4.7.7 The Contractor must provide full training for all assigned system users on how to maintain inmate alert levels and respond accordingly when these levels are exceeded.

✓ **Securus has read, understands, and complies.**

Authorized users will be trained in all system functions, including how to maintain inmate alert levels and respond accordingly when these levels are exceeded.

- 4.7.8 The Contractor must provide full training on the provided video visitation recording function including the live monitoring of visitation sessions, playback of visitation sessions and the transfer of visitation sessions to other media for playback at off-site locations.

✓ **Securus has read, understands, and complies.**

Authorized users will be trained in all system functions, including the recording function, the live monitoring of visitation sessions, playback of visitation sessions, and the transfer of visitation sessions to other media for playback at off-site locations.

- 4.7.9 The Contractor shall provide full training for all assigned MCSO system users on how to change inmate restriction levels (by kiosk, suspend PIN, etc.).

✓ **Securus has read, understands, and complies.**

Authorized users will be trained in all system functions, including how to change inmate restriction levels (by kiosk, suspend PIN, etc.).

- 4.7.10 The Contractor must provide full training for all assigned system users on how to initiate system restrictions.

✓ **Securus has read, understands, and complies.**

Authorized users will be trained in all system functions, including how to initiate system restrictions.

- 4.7.11 The Contractor must provide ongoing system training for existing MCSO personnel when required by the MCSO at no cost.

✓ **Securus has read, understands, and complies.**

Authorized users will be trained in all system functions at no cost to MCSO.

- 4.7.12 The Contractor must provide additional training for new MCSO personnel when required by the MCSO at no cost.

✓ **Securus has read, understands, and complies.**

Securus will provide training for new personnel when required.

- 4.7.13 The Contractor must describe, in its response, any advanced system training that may be available to MCSO personnel whether provided on-site at the MCSO facility.

✓ **Securus has read, understands, and complies.**

Securus can provide advanced training for Maricopa County personnel who will use additional administrative capabilities, such as determining who is watching or opening video files and for enhanced investigative capabilities. Securus will deliver the level of training required by Maricopa County.

- 4.7.14 The Contractor must provide a "live" Help Desk support function to MCSO at no cost to the MCSO during the term of this contract. This Help Desk function must be capable of providing support via telephone to the MCSO Web-based Video Visitation/Communication Kiosk System personnel for the functions of the Web-based Video Visitation/Communication Kiosk System. This "live" Help Desk must be available 24 hours a day, 7 days a week, 365 days per year.

✓ **Securus has read, understands, and complies.**

Securus is the only corrections industry provider that has made a strategic decision to centralize management of all technical services support. We provide superior customer service capabilities from a state-of-the-art technical service support center located in the metropolitan Dallas, Texas, area at 3000 Kellway Drive Suite 150; Carrollton, Texas 75006.

The TSC is staffed by approximately 50 technical center professionals and handles approximately 8,000 inbound queries per month. The TSC uses a call distribution system to automatically manage the flow of inbound customer calls. The TSC provides a single-point-of-contact where a facility may inquire on items such as remedial maintenance issue or trouble that may arise 24x7x365. Clients can contact the TSC by any of the following convenient methods to obtain service:

- **Telephone** – 866-558-2323
- **E-Mail** – technicalsupport@securustech.net
- **Fax** – 800-368-3168
- **Web portal** - <http://www.securustech.net/facility/Default.asp>

The technical service center offers the following features to our clients:

- Technical support and field dispatch 24x7x365
- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure Service Level Agreements are met
- Certified technicians to provide quick problem resolution
- Ownership of every issue via training, support, other departments, and historical information
- System and individual site connectivity monitored 24x7x365

24x7x365 Securus Technical Support Center



Securus technicians receive internal Securus certifications, based on our business and the products and services we support.

- 4.7.15 User Manuals - The contractor shall provide user manuals, both printed and electronic versions, for their platform to MCSO in sufficient number as deemed necessary by the Sheriff's Training Center.

✓ **Securus has read, understands, and complies.**

Securus will provide user manuals in sufficient numbers to MCSO.

4.8 REPORTS:

- 4.8.1 Ability to Customize Special Reports - The system may provide the capability to customize reports in a form mutually agreed upon by MCSO. This is a desirable feature. Please describe any categories in which this feature would be available.

✓ **Securus has read, understands, and complies.**

Securus offers standard reports for SVV but is willing to discuss with the County generating customized reports that meet your needs.

The SVV application and data reside on a server that is hosted on Securus' network. This server manages all the interactions between the SVV terminals and clients as well as provides secure storage of all data.

All the communications to and from the server are encrypted using military grade 256-bit encryption.

The SVV system is IP based and does not capture traditional telephone numbers; rather, it identifies the IP addresses of both parties in the session as well as the name of the visitor. SVV will allow Maricopa County to audit and report on all the activity of the system. Audit logs collect user information, IP address, date, type of activity, and short description (please refer to the examples below). The audit report can also allow filters based on date, type of message, user, etc.

Sample Audit Report

Proprietary and Confidential

Logs

Date:

Type:

User:

☐ Unknown

You could use wildcards (*) to start a filter. The search is made on database of logname and message.

Message:

Logs

User	IP address	Date (desc)	Type	Message
68.193.157.229	68.193.157.229	2011-08-17 20:41:16	Info	Logout
68.193.157.229	68.193.157.229	2011-08-17 20:39:38	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 18:23:16	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 17:02:54	Info	Logout
163.151.2.10	163.151.2.10	2011-08-17 17:01:58	Info	Appointment 720 created with "Scheduled" status (date: 2011-08-23, time: 13:00:00)
163.151.2.10	163.151.2.10	2011-08-17 17:00:51	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 16:56:51	Info	Appointment 719 created with "Scheduled" status (date: 2011-08-17, time: 17:00:00)
163.151.2.10	163.151.2.10	2011-08-17 16:56:45	Info	Logout
163.151.2.10	163.151.2.10	2011-08-17 16:53:49	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 16:13:32	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 15:09:14	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 15:05:44	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 15:00:10	Info	Logout
163.151.2.10	163.151.2.10	2011-08-17 14:51:00	Info	Appointment 718 created with "Scheduled" status (date: 2011-08-18, time: 13:00:00)
163.151.2.10	163.151.2.10	2011-08-17 14:37:40	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 14:09:39	Info	Appointment 717 created with "Scheduled" status (date: 2011-08-24, time: 14:00:00)
163.151.2.10	163.151.2.10	2011-08-17 14:06:09	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 13:48:33	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 13:20:01	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 13:05:15	Info	Appointment 716 created with "Scheduled" status (date: 2011-08-17, time: 13:30:00)
163.151.2.10	163.151.2.10	2011-08-17 12:26:16	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 12:21:50	Info	Login
163.151.2.10	163.151.2.10	2011-08-17 12:00:43	Info	Logout
163.151.2.10	163.151.2.10	2011-08-17 11:59:44	Info	Appointment 715 created with "Scheduled" status (date: 2011-08-17, time: 13:30:00)

SVV allows Maricopa County to generate usage reports for the system. These reports collect session ID numbers, appointment numbers, date, caller, inmate, session start, session end, and call duration, as shown below. The user report can also allow filters based on dates, user, or group.

Sample Report

Proprietary and Confidential

Report list

Date: 2011-08-16

2011-08-17

User:

You must be logged in (to view report) user. The search is made on username, password and institution

Group:

search

cancel

Report list

Session	Appointment	Date	Caller	Inmate	Start	End	Duration
3662	690	2011-08-16	F. [redacted]	[redacted]	14:40:49	14:40:49	0
3665	655	2011-08-16	C. [redacted]	[redacted]	14:44:14	14:44:14	0
3666	691	2011-08-16	F. [redacted]	[redacted]	18:32:08	18:50:22	18
3667	692	2011-08-16	F. [redacted]	[redacted]	19:01:11	19:16:05	14

24 results

Export to CSV

Print

Billable sessions are billed on a pay-per-use basis. Based on a user's profile, user will be asked to pay for a session when it is scheduled. All billing and credit card processing is managed by Securus. Pricing for sessions is determined ahead of time with the facility.

- 4.8.2 Finance Reports - The contractor shall list any and all reports available. Include an example of the reports. These should include revenue and commission by jail facility and category.

Securus has read, understands, and complies.

Maricopa County will be able to use our robust Facility Portal's stratification report to meet a majority of your reporting needs. Securus will work with the County to meet any needs for reports not currently available. An example of a call commission report, which includes a line for SVV commissions, is on the following pages.

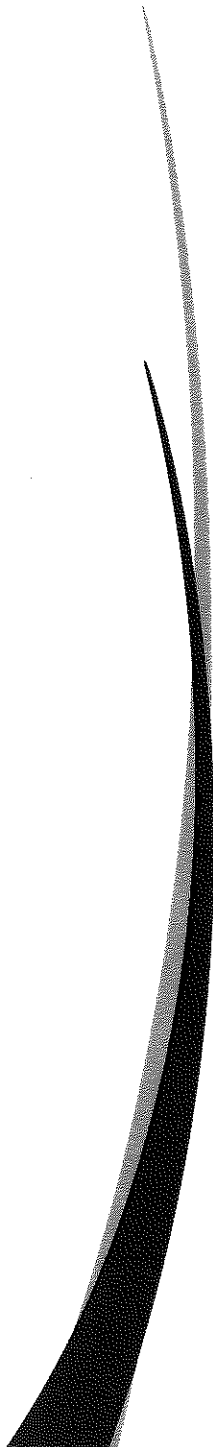
- 4.8.3 Maintenance Reports - The contractor shall list any and all reports available and include an example of each report. Each month the contractor will provide MCSO a report for each preceding month, to include:

4.8.3.1 Kiosk Repairs

Securus has read, understands, and complies.

Maricopa County will use the ticket (event) tracking feature from Facility Portal to determine maintenance that has been performed.

The Securus event tracking system logs, tracks, manages, and assures appropriate response to all service requests. The service request generates a unique trouble ticket number that is linked to each facility's service history and provides real-time updates. Each ticket has a priority level assignment, which drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem, and resolves the problem or engages the appropriate party for problem resolution.



SECURUS
SECURITY SOLUTIONS

**Solicitation # 13002-RFP Web-Based Visitation/Communication
Kiosk System**

© 2013 Securus Technologies, Inc. All rights reserved.

5.20.4 Proposal



**Solicitation # 13002-RFP Web-Based Visitation / Communication
Kiosk System**

© 2013 Securus Technologies, Inc. All rights reserved

4.8.3.2 Web-based Video Visitation/Communication Kiosk System Trouble Tickets

✓ **Securus has read, understands, and complies.**

Securus provides partnering facilities like Maricopa County with one of the only web-based, anywhere, anytime single-point access customer portals in the industry. At any time, day or night, 24x7x365, Maricopa County can securely access details about your facility's operations. Approved users can access all calling activity, including all call detail reports.

The Facility Portal can serve as the user interface to Securus' electronic trouble ticket system and allows authorized users to perform functions such as creating and managing service tickets and generating reports. With Facility Portal, users can initiate trouble tickets for repairs, track the real-time status, and generate current and historical reports of these tickets. After a ticket is generated, a tracking number is automatically and immediately created. All updates are sent in real-time electronically to the originator of the ticket, as well as to the County designee.



Facility Portal Service Center

The Service Center will allow the user to create and manage their facility's technical support tickets. As needed, users can search for service tickets by entering the ticket number in the search field or by selecting date search

The following figure provides an example of the screen used to manage service tickets.

Manage Your Service Tickets

Proprietary and Confidential



FRIENDS & FAMILY CORRECTIONAL FACILITIES ABOUT US CAREERS CONTACT US

Facility Portal

Facility Name

Dashboard

Portal Manager

Commissions Reports

General Reports

Order Materials

Downloads & User Guide

Service Center

Your Tickets

Create A Ticket

Date Search

Search Tickets

Help

Secure Call Platform

Log-Out

Your Service Tickets

SITE NAME	TICKET #	DESCRIPTION	LAST UPDATED	STATUS
Facility Name	13802698	Div 11 VB enrollments	2011-08-16 09:56:04	Closed
Facility Name	13799289	Voice Biometrics - the customer is enrolling/re-enrolling inmates in VB at Division 11...	2011-08-12 11:06:18	Closed
Facility Name	13792501	Report Request: Calls completed in 2008 from Division 1, Tier B-4 Call period is 9/1...	2011-08-05 15:19:43	Closed
Facility Name	13783054	customer reports that he creates an iso image to burn to DVD and when image was downlo...	2011-07-29 10:24:54	Closed
Facility Name	13782536	Voice Biometric - Re-enrollments the customer is doing re-enrollments of inmates at t...	2011-07-28 11:10:58	Closed

1234
Total Tickets

By clicking on the ticket number, a detailed report pops up. If a ticket is closed, you can review all the previous notes and the final resolution at any time. If the ticket is currently open, you can create a new journal note. Consent to close a ticket can also be performed using the notes section.

The following figure provides an example of ticket detail.

Ticket Detail

Proprietary and Confidential



Facility Portal

Marketing

- Callboard
- Email Manager
- Reports
- Order Materials
- Downloads & User Guide
- Service Center
- Hour Tickets
- Check & Troubleshoot
- Data Manager

Search Tickets

Go

Go

Ticket Details #13529104

Ticket Progress

Case Description: Remote paid to block phone not working

Ticket Priority: 3

Ticket Status: Closed

Date Opened: 12/28/2013 @ 14:24 AM

Last Update: 12/28/2013 @ 01:24 AM

Solution Description: Asset sig.

ASSIGNED TO: TERRY S

Issue	Date	Issue Resolved - Waiting for Customer Approval
Issue	12/28/2013 @ 14:24 AM	Issue Resolved - Waiting for Customer Approval
Issue	12/28/2013 @ 14:24 AM	Issue Resolved - Waiting for Customer Approval

View All Tickets

Our on-site technical support personnel can assist in the tracking and reporting of service tickets to alleviate extra work from MCSO staff.

4.8.3.3 System Reboots

✓ **Securus has read, understands, and complies.**

Securus logs system reboots and, should Maricopa County require, can be notified of instances when these occur.

4.8.3.4 System Upgrades

✓ **Securus has read, understands, and complies.**

Maricopa County will be notified beforehand of all system upgrades and when they are scheduled to be implemented. System upgrades, allowing for additional capabilities to be uploaded to the visitation system interface, are regularly provided at no cost to our customers. In much the same

way as our inmate calling system, our video visitation technology is designed to evolve and be future proof.

- 4.8.4 Inmate Reports - The contractor shall list any and all reports available and include an example of each report. (An example would include video specific to one inmate by time and date.)

✓ **Securus has read, understands, and complies.**

Maricopa County can use SVV's sample report, displayed earlier in this section, and filter such details as user or user group type to show different visitation details.

- 4.8.5 IP Number Reports - The contractor shall list any and all reports available and include an example of each report. (Examples may include blocked IP numbers, IP numbers visiting more than one inmate, and frequently used IP numbers.)

✓ **Securus has read, understands, and complies.**

Because IP addresses can be seen in report details, SVV has the ability to log all visits, including information such as times inmates used the system and who they visited with, and the IP address visited.

- 4.8.6 Web Video Access Reports - The contractor shall list any and all reports available and include an example of the reports.

✓ **Securus has read, understands, and complies.**

Standard reports can be filtered by such variables as user and user group type, including remote users on the web.

- 4.8.7 Investigative Reports - The contractor shall list any and all reports available and include an example of each report.

✓ **Securus has read, understands, and complies.**

Securus will work with Maricopa County to identify and meet future reporting needs. In addition, Maricopa will be able to use the THREADS™ investigative lead generator to help solve crimes. THREADS is a powerful, accurate, and extremely easy to use software application that will automatically generate leads for investigators by uncovering calling patterns, associations between multiple offenders, and their correlation to called parties.

THREADS will automatically analyze investigative data such as offender communication records, public phone records, and data from confiscated cell phones to generate focused leads for

investigators. Leads can include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple offenders, their correlation to called parties, and much more.

4.8.8 Inmate Email Reports- The contractor shall list any and all reports available and include an example of each report.

✓ **Securus has read, understands, and complies.**

Securus proposes to operate its Secure Instant Mail (SIM) application on the SVV terminal, giving inmates another way to communicate with friends and family and Maricopa County both an additional source of revenue and a tool that investigators can use to solve crimes.

Secure Instant Mail is similar to standard email but built for the corrections environment, meaning it was designed to be flexible, secure, efficient —and profitable for the county.

4. Account Setup and Sending Email

The inmate's friend or family member sets up a Secure Instant Mail account by going to www.securustech.net. Using the Secure Instant Mail website, they can select the facility and inmate receiving the email, compose the email, select messaging options, pay for the email and send the email. Messaging options include requesting approval notifications, prepaying for inmate responses, and even uploading pictures. The email is then processed through the system for the facility's approval before it is sent to the inmate.

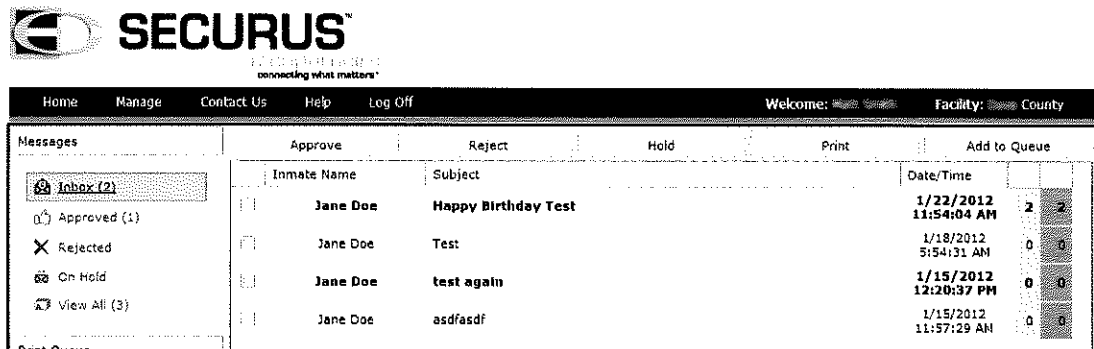
5. Facility Approval

Authorized facility staff logs into the facility's Secure Instant Mail website with a secure user name and password to manage inmate emails. Staff can review, approve, and reject emails and pictures. This process is simplified through a customizable **automatic word search engine**, which flags illicit and potentially illicit words in the emails.

The following figure illustrates the system's capability to flag pending emails that contain word warnings. Their critical relevance is indicated as "red" or "yellow." The facility staff can easily point and click for approval or rejection from any approved PC at anytime, anywhere.

Secure Instant Mail Inbox with Red and Yellow Warning Word Indicator

Proprietary and Confidential



Once the email is approved, it is archived and can be distributed to the inmate. If the friend or family member has selected to be notified, they would receive an automatic reply email at this time, confirming the approval.

6. Delivery to the Inmate

Maricopa County inmates will receive the email through optional methods including print format and by accessing a Securus Video Visitation kiosk (if available in the facility). Inmates may reply to their email through kiosks or by submitting their written response to facility staff to be approved and scanned into the system to be sent via email to the friend or family member.

Improving Maricopa County Operations Through Automation and Innovation

Secure Instant Mail was not only designed to provide Maricopa County with additional revenue, but also to improve mail room operations security and efficiency. This is accomplished through fully integrated technology that places all automated tools needed to create, approve, send, and receive, and respond to email in the hands of the users.

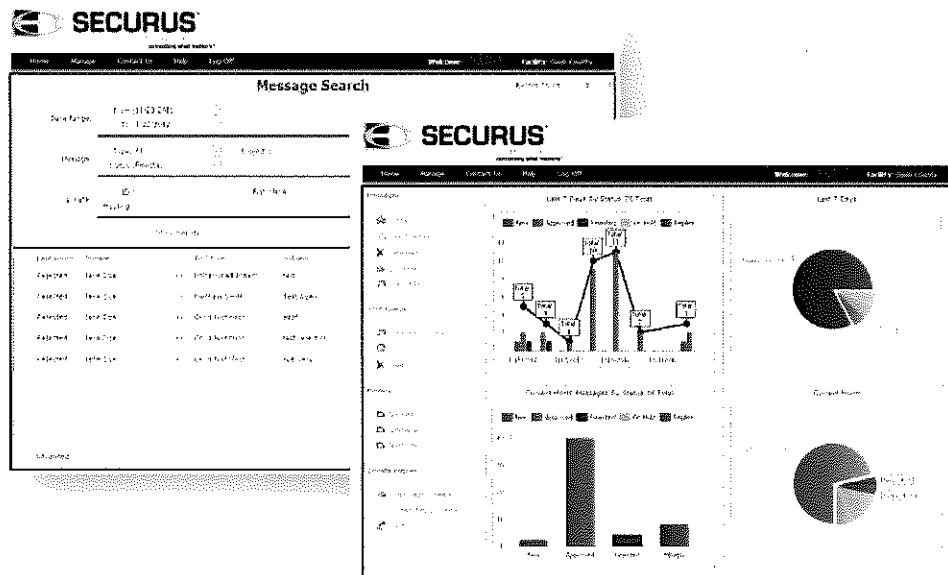
Use of Secure Instant Mail includes the following benefits:

- Eliminates the need to open, analyze, sort, translate, or x-ray mail.
- Reduces contraband, improving the safety of facility officers as well as inmates.
- Speeds up the emails approval process through integrated word search engine with a built-in, editable dictionary.
- Enhances investigations by archiving each email in a secure centralized database. Through the Secure Instant Mail website, investigators can search for emails by inmate, sender, date range, keyword, and much more.

- Provides an interactive dashboard of email traffic by type, status, and date—giving administrators a complete email management tool right at their fingertips.

Secure Instant Mail Message Search and Interactive Dashboard

Proprietary and Confidential



The Dashboard in the image above on the right reports a visual representation of email activity within the last seven to 30 days. This is the fastest and easiest way to monitor activity and ensure you are getting the very most out of this powerful product. To access the Dashboard, simply highlight "Manage" in the upper navigation bar and select "Dashboard."

- 4.8.9 Inmate Tank Order Reports- The contractor shall list any and all reports available and be able to differentiate between requests (i.e. programs, religion, library, ILS). Include an example of each report.

✓ **Securus has read, understands, and does not comply.**

Maricopa County can use SVV's sample report, displayed earlier in this section, to filter details and show different visitation information or request details by inmate.

4.8.10 Disciplinary Action Reports- The contractor shall list any and all reports available and include an example of each report.

✓ **Securus has read, understands, and does not comply.**

Securus prides itself on being a partner to our customers and providing high-quality services that meet their needs. We look to improve our services and products based on customer demand, and as a flagship account (should we be selected to provide Maricopa County's video visitation services) we would work with you to fully understand your needs and enhance SVV to create such reports.

4.9 PERFORMANCE SPECIFICATIONS:

Disputes/Fines/Assessments - MCSO expects the contractor to fully comply with the time frames in this contract. However, should a dispute arise as to whether there should be a fine for non-compliance and if so, how much, the dispute will be resolved by a team consisting of two (2) members from MCSO, one (1) member from Maricopa County Office of Procurement Services Department and one (1) member from each of the contractors service team. Each dispute resolution team member will have one vote with the exception of the service provider team member whose company is being considered for assessment of the fine. This exception team member may represent his company's position during the discussions. A simple majority shall be required of the eligible voting dispute resolution team members to determine the resolution. The decision will be based on the logbooks, work orders, e-mails, and written explanations from all parties involved in the dispute. The final decision of the dispute resolution team will be final and binding upon all parties.

✓ **Securus has read, understands, and complies.**

4.9.1 Jail Facility Access Security Clearance - MCSO does not allow a service contractor access into a jail facility to perform any type of service unless a background check has been completed, per Exhibit 7 Jail Access Policy. The MCSO Facilities Security Guidelines (Exhibit 7) explain all the necessary requirements of contractors performing work at such facilities. If it is anticipated that the contractor has staff visiting the site on a consistent basis, these forms will be completed by the person requesting facility access and the background check will be completed prior to approving access. Once the form is filled out and submitted to MCSO, the contractor shall be notified if approved and a jail access identification card will be issued.

✓ **Securus has read, understands, and complies.**

4.9.2 Security of Records/Recordings - The contractor shall provide adequate security of the inmate Web-based Video Visitation/Communication Kiosk System records and recordings. Access to the Web-based Video Visitation/Communication Kiosk

System records and recordings will be limited to those employees of the contractor who requires the information to properly perform services for MCSO.

✓ **Securus has read, understands, and complies.**

Securus provides multiple safeguards, both at a user and facility level, to ensure the highest amount of security for at home visitation. In addition to a registration process which requires end users to enroll and take verification photographs of their identification and profile, which must be approved prior to a visit being scheduled, Securus takes the following steps to ensure security:

- Video security screens which do not permit viewing at an angle
- Hardened glass on terminal screens to minimize breakage and downtime
- Ventilated and cooled video monitor hardware without providing inmates areas to "stuff" items
- Magnetic on and off switch to prevent inmate tampering
- Vandal proof handset with armored cable
- Assembly elements are hidden: No screws or hinges can be removed and used to manufacture weapons. No doors/compartments that can be opened in the front or on the sides of the unit
- Rounded edges that reduce the risks of accidental or intentional injuries
- Abrasion and chemical resistant; can be cleaned with commercial cleaners without damage
- Live monitoring capabilities of real-time visits
- Recording of visits for security purposes
- Impact Resistance - Meets UL-60950 and CSA 22.2 No. 60950 ball drop test (0.5kg, 50mm diameter ball dropped from height of 1.3m)
- Screen size is 15"
- Terminal has steel, mounting bracket which is bolted to the wall. Afterwards, the terminal is secured to the bracket.
- Light and ruggedized vandal-proof terminals (constructed with hardened, cold rolled steel .075/14 gauge): Best balance between weight and resistance
- Terminal is sealed: Minimize dust and liquid entry, spill proof, completely sealed front, spill-resistant back with openings to allow heat to escape.
- Hidden magnetic activated pushbutton for on/off power
- Built-in heat sink at the back for heat dissipation
- Power: 110V; 2AMP
- All content is delivered via web browser through servers hosted in Securus' data centers.

In addition, the Maricopa County's VVS network will operate on Securus' secure, private network.

Securus understands the importance of security, particularly in the corrections industry and takes security concerns seriously.

Securus applies a high level of security to protect against cyber-pirates. Applications transmitting data across public networks are supporting SSL, Certs, and encryption. Cisco and Juniper firewalls, used throughout the network to protect SCP and our customers, create DMZ networks. In addition, all servers, laptops, and workstations require anti-virus and anti-spyware protection software, and the latest operating system patches. Securus supports both AVG and Symantec anti-virus.

From a physical security standpoint, SVV is co-located in a carrier-class data center that has some of the most comprehensive security measures in the telecommunications industry. Access to network facilities is controlled through multiple levels of mandatory physical security.

Security personnel maintain the following procedures for allowing entry into the data centers:

- Security personnel are on premise 24x7x365.
- Cardkey reader (electronic badge).
- Identification badges are issued to all persons having a business need to access Company premises.
- Man traps are located at each entry/exit point in the data center. Man traps use two sets of doors that require electronic badge entry. The first set of doors must close before the second set will open.

All visitors, customers, contractors, and repair personnel must gain access from the security officer on duty.

Customers, contractors, repair personnel, maintenance personnel, and non-local employees may access buildings and critical areas at all times, if there is an escort. Vendors may access buildings and critical areas only during working hours, if there is an escort.

As Securus has demonstrated with over 25 years of call platform enhancements, we will continue to reinvest in our video platform over the term of our relationship to implement features driven by our customers. As new advances in security are made available, we will provide them to Maricopa County.



- 4.9.2.1 Procedures and Controls - The contractor shall establish and maintain procedures and controls that are adequate to assure that no information contained in its records and/or obtained from the Sheriff's Office or from others in carrying out the functions/service under this Agreement shall be used by or disclosed by it or its employees, except as required to efficiently perform duties under the Agreement.

✓ **Securus has read, understands, and complies.**

Securus enforces rigorous processes and procedures to ensure we maintain the proper level of control over all customer information. Securus claims the distinction of being the only inmate communications provider who has earned SOC-1 certification; SOC-1n formerly known as SAS-70 Type II, certification, is issued by the American Institute of Certified Public Accountants Statement on Auditing Standards No. 70 (SAS 70). A SOC-1 certification indicates that an independent accounting and auditing firm completed a comprehensive and in-depth evaluation and testing of Securus' internal controls and related activities. This certification confirms that the company has effective controls and safeguards in place to manage information and data belonging to its customers. Because inmate telecommunications providers, like Securus, need to install and operate highly sophisticated call management platforms and related services to meet the security and public safety needs of correctional facilities, we need to be able to accurately process, manage, and control millions of call records and call recordings for security and investigative purposes. An SOC-1 report reinforces to correctional facilities and their auditors that Securus has the necessary controls in place to manage this critical information.

No other video visitation or inmate communications vendor has been granted SOC-1 certification except Securus.

4.9.2.2 Records/Recordings Confidentiality - Contract employees that have access to the inmate telephone records and recordings shall be required, at a minimum, to sign a Non-Disclosure/Confidentiality Agreement and potentially the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum Certification.

✓ **Securus has read, understands, and complies.**

4.9.2.3 Records/Recordings Security Clearance - Contract employees that have access to the inmate video records and recordings shall be required to complete, at a minimum, a background check and potentially a fingerprint check.

✓ **Securus has read, understands, and complies.**

Securus very rarely uses contract employees, preferring to trust your sensitive information and communications between inmates and their friends and families with our employees. Securus has approximately 700 employees serving our customers and, unlike most vendors, deploys contractors only when a Securus employee is not available.

4.9.2.4 Legal Video/Web-based Visitation shall not be recorded without a court order.

✓ **Securus has read, understands, and complies.**

Securus understand and respects attorney-client privilege and abides by all laws to ensure that sessions are not recorded.

4.9.3 Trouble Ticket Fines

4.9.3.1 Priority Level One (1) Fine: A fine of \$500.00 shall be assessed to the contractor for every day in which a Priority Level One (1) Trouble Ticket has not been resolved and the service is not fully restored to the affected areas.

✓ **Securus has read, understands, and complies.**

4.9.3.2 Priority Level Two (2) Fine: A fine of \$250.00 shall be assessed to the contractor for every day in which a Priority Level Two (2) Trouble Ticket has not been resolved and the service is not fully restored to the affected area.

✓ **Securus has read, understands, and complies.**

4.9.3.3 Priority Level Three (3) Fine: A fine of \$100.00 per day shall be assessed to the contractor for every day in which a Priority Level Three (3) Trouble Ticket has not been resolved and the service is not fully restored to the affected area. A 48-hour grace period will apply.

✓ **Securus has read, understands, and complies.**

4.9.4 Compliance of Jail Access Rules and Regulations - The contractor shall comply with all provisions outlined in MCSO Policy DH-1, Jail Access (Exhibit 7).

✓ **Securus has read, understands, and complies.**

4.9.5 Staffing

4.9.5.1 On Site Technicians - The contractor shall provide three (3) full-time "on-site" technicians at their expense to provide service. The technicians must have at least two (2) years of related experience, to include installing, maintaining, testing, and repairing voice and data communications systems and equipment. The duties include:

✓ **Securus has read, understands, and complies.**

Securus will provide on-site technicians required to fully support the Maricopa County Jail's video visitation needs.

4.9.5.1.1 Repair and Maintenance - The contractor shall provide service for all Web-based Video Visitation/Communication Kiosk System repair and maintenance.

✓ **Securus has read, understands, and complies.**

Securus supports the use of video visitation as a viable, cost-effective technology to enhance communications between inmates and their friends and families, and as a source of both information for investigators and revenue for MCSO. Therefore, an integral part of our mission is to keep terminals operating at full capacity to accomplish these goals.

4.9.5.1.2 Video Party Billing Issues - The contractor shall handle all billing issues from the parties called by the inmates.

✓ **Securus has read, understands, and complies.**

Securus will handle all billing issues and provides all billing services internally through Securus Correctional Billing Services (SCBS). Our ability to produce our own billing allows us to offer the most robust video visitation program in the industry. More sessions mean more revenue and commissions.

4.9.5.1.3 Complaints - The contractor shall handle all complaints from the parties for web-based issues.

✓ **Securus has read, understands, and complies.**

Securus is unique among its national competitors in offering an in-sourced call center located in the Dallas metropolitan area to provide customer service to friends and family members of inmates. Our 200+ seat call center employs customer service representatives who are trained and managed by Securus management.

Live agent support is available to friends and family members 7 days a week, 24 hours a day, and 365 days a year.

Customers can use our toll-free number (1-800-844-6591) to either speak to a "live" agent, or to take advantage of our easy to use automated system to help them with their needs. For added convenience, we also offer personal account access via our website (www.securustech.net) or via e-mail (customer_service@securustech.net).

Also end-users may now access SCBS' customer service via chat 24 hours a day, seven days a week.

4.9.5.2 Trained Support Staff - The contractor shall maintain properly trained support staff on the Web-based Video Visitation/Communication Kiosk System.

✓ **Securus has read, understands, and complies.**

Securus provides comprehensive training to each employee in the company. We seek the best employees to join our team. While searching for new staff, Securus looks for CCNA, MCSE, MCP, MCDBA, A+, Net+, or other industry standard Telecommunications certifications and experience.

All Technicians hired or transferring into Technical Support are sent through Securus' Level 1 Training led by our in-house training department. To advance through Technical support, additional training is required and provided by our training department and Technical Support's most senior technical support staff.

While based on industry standard hardware and protocols, our unique complex architecture requires we provide instructor-lead courses specific to many of our applications. Much of this training is delivered by Technical Support's highly skilled senior subject matter experts who are regularly briefed on the latest product advancements directly by our Development Engineers.

As part of our ongoing commitment to our staff's continuing development, we introduced a learning initiative that can be accessed from the staff's desktop computer. Our goal is to support our staff's continuing development through innovative online learning that can be accessed 24 hours a day, 7 days a week. With our online learning program, our staff members have access to a diverse library of content. These courses cover a wide variety of subject matter to meet the various training needs of all our associates from highly technical industry standard topics to our proprietary software application instructions. Securus also funds continuing higher education from public and private universities that award academic degrees or professional certifications.

Additionally, our SCBS associates receive in-depth product and customer service training so they can deliver professional, insightful assistance when inmates' friends and families call for any issue.

4.9.5.3 Compliance of Code of Conduct for On Site Technicians - The On-Site Technicians shall comply with all provisions outlined in MCSO Policy CP-2 Code of Conduct (Exhibit 6).

✓ **Securus has read, understands, and complies.**

4.9.5.4 Replacement of On-Site Technicians - The contractor shall replace any on-site administrator who leaves employment with the contractor, within twenty-one (21) days. This replacement may be a temporary or

permanent employee. If the replacement is a temporary employee, a permanent employee (full or part-time) will be hired by the contractor and on site within sixty (60) business days of the date the previous employee left employment of the contractor.

✓ **Securus has read, understands, and complies.**

4.9.5.4.1 Fine - Failure to comply shall result in a \$250.00 fine per day until the contractor is in compliance.

✓ **Securus has read, understands, and complies.**

4.9.6 Service Point of Contact - The contractor shall provide a complete list of business telephone numbers, emergency telephone numbers, addresses, and e-mail addresses of the contractor's managers, administrators, and technicians within ten (10) days of the award of the contract.

✓ **Securus has read, understands, and complies.**

4.9.7 Public Complaints Point of Contract - The contractor shall provide a single point of contact for any and all public complaints regarding telephone service. This service must be provided for both English and Spanish speaking individuals.

✓ **Securus has read, understands, and complies.**

Friends and family members can call our SBCS call center 24 hours a day, 7 days a week to resolve any issues regarding Securus' service. Our associates can help callers in either English or Spanish.

4.9.8 Complaints of or by Contracted Employees - The contractor shall investigate any complaints of or by contracted employees and have resolution within thirty (30) days with notification of such to MCSO.

✓ **Securus has read, understands, and complies.**

4.9.9 Office Equipment - Any office equipment, desks, cell phones, pagers, etc., required by the contractor's personnel shall be the responsibility of the contractor.

✓ **Securus has read, understands, and complies.**

- 4.9.10 Remote and On-Site Monitoring - The contractor shall provide to MCSO on-site monitoring during normal business hours and remote monitoring and diagnostic service, twenty-four (24) hours a day, seven (7) days a week.

✓ **Securus has read, understands, and complies.**

SVV is constantly monitored by Securus employees from our NOC at our headquarters location in the metropolitan Dallas, Texas, area. This service center is staffed 24x7x365 by network experts who are certified in the systems and software used to monitor all SCP functions and equipment, as well as the associated network. The NOC maintains failure reports, service history, and other diagnostic information, which will be available to the County when requested.

The NOC will maintain the names and contact information for each Securus employee supporting Maricopa County. They will be accountable for any actions required to prevent or repair any outages. Securus will follow the County's protocols for communicating outages or repair actions in the unlikely event these occur.

Securus Network Operations Center in Dallas, TX



Premium Network Monitoring Capabilities

Securus proactively identifies potential system and network abnormalities through a centralized diagnostic application, Orion by Solar Winds. This network management software allows Securus personnel to continuously monitor all hardware, software, and system metrics.

Through our network monitoring practices, we are able to complete the following functions:

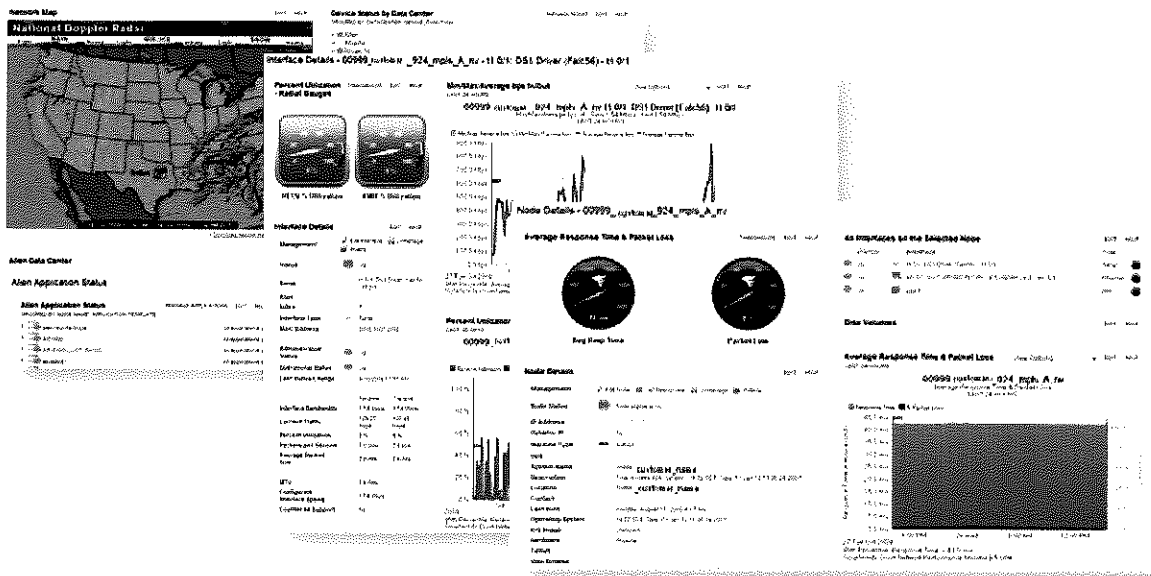
- **Enable proactive repairs to a system to prevent it from going down.** Many times corrections are made before a system shows signs of an issue and before the facility is aware of a problem. This means less down time and increased system reliability for the facility.
- **Alert remote or on-site engineers of any system threshold inconsistencies or alarms.** If detected:
 - Alerts are sent to the NOC to track the event.
 - The NOC communicates with engineers through email, short message service (SMS), or directly through a wireless phone to address the issue.
- **Receive real time alerts when the system detects an error.**
 - Identifies if the network elements health threshold has been exceeded or if any other potential system issue has been discovered.
 - Establishes volume thresholds for each transport carrier on core node equipment at each data center, alerting Securus personnel of possible carrier network issues.
- **Monitor call traffic patterns, bandwidth detail, and network life cycle management to ensure sufficient resources are in place.** A separate capacity engineering team reviews call traffic volume reports and storage requirements throughout all systems.
- **Centrally monitor all calling traffic and reporting to determine if increase or decreases in the number of telephones are needed.** Upon agreement by the County, the service and operations team will install any additional telephones required.

Remote Programming, Diagnostics, and Troubleshooting

The Securus NOC uses the Orion network monitoring application to constantly check the system to ensure optimum performance and to anticipate the need for additional network or capacity.

Visual monitoring in our NOC is achieved through the use of several key screens that are constantly updated and monitored by our personnel in our NOC.

Sample Network Operations Center Monitoring Screens



The NOC can contact the Technical Support Center (TSC) if it determines that another level of technical support may be needed to address issues or concerns. This action could involve dispatching a Field Services Technician to a Maricopa County facility.

A description of our next team, the Technical Support Center, follows and continues to demonstrate the importance of our integrated teams.

Technical Service Center

Securus is the only corrections industry provider that has made a strategic decision to centralize management of all technical services support. We provide superior customer service capabilities from a state-of-the-art technical service support center located in the metropolitan Dallas, Texas, area at 3000 Kellway Drive Suite 150; Carrollton, Texas 75006.

The Securus Technical Services Center (TSC) is staffed by approximately 50 technical center professionals and handles approximately 8,000 inbound queries per month. The TSC uses a call distribution system to automatically manage the flow of inbound customer calls. The TSC provides a single-point-of-contact where a facility may inquire on items such as remedial maintenance issue or trouble that may arise 24x7x365. Clients can contact the TSC by any of the following convenient methods to obtain service:

- **Telephone** – 866-558-2323
- **E-Mail** – technicalsupport@securustech.net

- **Fax** – 800-368-3168
- **Web portal** - <http://www.securustech.net/facility/Default.asp>

The technical service center offers the following features to our clients:

- Technical support and field dispatch 24x7x365
- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure Service Level Agreements are met
- Certified technicians to provide quick problem resolution
- Ownership of every issue via training, support, other departments, and historical information
- System and individual site connectivity monitored 24x7x365

24x7x365 Securus Technical Support Center



Securus technicians receive internal Securus certifications, based on our business and the products and services we support.

- 4.9.11 System Checks and Preventative Maintenance - The contractor shall perform system checks and preventative maintenance on a monthly basis to ensure the system is operating at optimum efficiency and performance.

✓ **Securus has read, understands, and complies.**

The NOC monitors the network 24 hours a day, seven days a week and performs all remote diagnostics and maintenance possible. Any required on-site maintenance will be conducted by the on-site technicians augmented by Securus Field Services staff.

- 4.9.12 Coordination of Services - All changes in present and future services shall be coordinated with the Web-based Video Visitation/Communication Kiosk System Manager, or designee.

✓ **Securus has read, understands, and complies.**

Darrin Hays, dhays@securustech.net or (480) 717-8790, is the Account Manager assigned to ensure that Maricopa County receives the best possible service from Securus. Darrin will coordinate all system updates and future service needs with Maricopa County's Web-based Video Visitation/Communication Kiosk System Manager, or designee.

- 4.9.13 Coordination of Maintenance - All operational maintenance shall be coordinated with the Web-based Video Visitation/Communication Kiosk System Manager, or designee.

✓ **Securus has read, understands, and complies.**

Darrin Hays or the on-site technicians, whomever is most appropriate, will coordinate all operational maintenance with the Web-based Video Visitation/Communication Kiosk System Manager, or designee.

- 4.9.14 Kiosk Cleaning at Time of Service - All exterior of equipment as well as interior and exterior enclosures shall be cleaned at the time of each service. Labels or information cards will be replaced when missing or damaged.

✓ **Securus has read, understands, and complies.**

- 4.9.15 Clean Up and Debris - The contractor shall clean up and remove all debris and packaging material resulting from work performed.

✓ **Securus has read, understands, and complies.**

- 4.9.16 Project Plan - The contractor shall provide a detailed project plan, including a Gantt Chart, stating all tasks, milestones, and target dates for the initial project.

✓ **Securus has read, understands, and complies.**

Please refer to Appendix A for Securus' preliminary implementation schedule. The schedule will be finalized with input and approval from Maricopa County's Web-based Video Visitation/Communication Kiosk System Manager, or designee and any other stakeholders you require.

- 4.9.17 Statement of Work - The contractor shall provide a statement of work and obtain MCSO approval for any and all software changes prior to the installation of the software change.

✓ **Securus has read, understands, and complies.**

The architecture of SVV is built to implement software upgrades in real time, limiting disruption to the service. As new features are available, they are added to the central processor, making them available to all facilities. If service has to be disrupted for an upgrade, the upgrade will be conducted between the hours of 11 p.m. and 7 a.m.

Your Territory Manager, Darrin Hays, who is dedicated to your account, will communicate when new features are available and will schedule additional training, if needed.

- 4.9.18 Installation, Replacement, and Repair Cost - The contractor shall be responsible for installation, replacement, and repair cost of all equipment due to any reason including, but not limited to, vandalism, normal wear and tear, and new installation requirements.

✓ **Securus has read, understands, and complies.**

- 4.9.19 Cost of Installation, Monthly Usage and Maintenance of Kiosks - All expenses involved with the installation, monthly usage, and maintenance of the contractor-installed telephone lines shall be borne solely by the contractor.

✓ **Securus has read, understands, and complies.**

- 4.9.20 Credit and Collection Practices - The contractor shall adhere to reasonable credit and collection practices.

✓ **Securus has read, understands, and complies.**

4.10 RATE AND COMMISSION STRUCTURE:

- 4.10.1 Please provide information on the rate structure for video visitation sessions. Include within your response the cost per sessions for attorney, friends, and family visitors.

✓ **Securus has read, understands, and complies.**

- 4.10.2 Web-based Rates - Fair and reasonable rates to the families of inmates are an important part of the Web-based Video Visitation/Communication Kiosk System.

✓ **Securus has read, understands, and complies.**

Securus helps make connecting through video visitation sessions as easy and inexpensive as possible for friends and family as well as others such as attorneys and does not charge an enrollment fee to schedule sessions. Securus proposes to provide the first month of service free to entice users to register and get comfortable with the system, its features, and capabilities. Thereafter, each session will cost visitors only \$12.95 plus taxes and fees for a 20-minute visitation session.

In developing its SVV product, Securus conducted a formal survey and found most friends and family members would pay between \$10 and \$20 for a video visitation session when compared to "typical" costs of physically visiting a facility of up to \$31.50 for travel and three hours lost wages. In addition, 93 percent of those surveyed said they have a computer and Internet access and 66 percent of the remainder said they could get that access.

- 4.10.3 Notification of Rate Changes - MCSO shall be notified in writing of any proposed increases or decreases in the rates charged.

✓ **Securus has read, understands, and complies.**

- 4.10.4 Detailed Pricing Structure - Provide a detailed pricing structure for all types of calls. Identify all surcharges, administrative fees and per minute fees associated with all types of web-based visits and inmate email specified in this contract.

✓ **Securus has read, understands, and complies.**

- 4.10.5 Commission Payment(s) and Accountability

- 4.10.5.1 The commission offered to MCSO shall be based on total gross revenues (as outlined in the detailed pricing structure), with no deductions for fraud, bad debt, uncollectible, or un-billable calls. No deduction shall be made for any cost of providing the service(s) described.

✓ **Securus has read, understands, and complies.**

- 4.10.5.2 Commissions shall be paid monthly and sent to:

Maricopa County Sheriff's Office
234 N. Central Avenue, 7th floor
Phoenix, AZ 85004
Attn: Financial Services Division

✓ **Securus has read, understands, and complies.**

Securus will begin paying commission after the system is paid off. Commission checks will be paid monthly and sent to the above address.

4.10.5.3 Payment shall arrive no later than thirty (30) days following the calendar month for which commissions are being paid. Failure to submit commissions within sixty (60) days following the billing month gives the County the right to impose and collect interest at the maximum legal rate for all late payments.

✓ **Securus has read, understands, and complies.**

4.10.5.4 Failure to pay accurate commissions on a regular, monthly basis shall be grounds for cancellation, without penalty, of agreement executed as a result of the RFP.

✓ **Securus has read, understands, and complies.**

4.10.5.5 A monthly commission and summary report that includes, at a minimum, the following information shall to be sent to the Web-based Video Visitation/Communication System Manager: date of report, time period covered, total number of calls by category, total number of minutes by category, total gross revenue (as defined above).

✓ **Securus has read, understands, and complies.**

4.11 ACCEPTANCE:

Upon successful completion of the performance period, the system shall be deemed accepted and the warranty period begins. All documentation shall be completed prior to final acceptance.

✓ **Securus has read, understands, and complies.**

4.12 FACILITIES:

During the course of this Contract, the County shall provide the Contractor's personnel with adequate workspace for consultants and such other related facilities as may be required by Contractor to carry out its obligation enumerated herein.

✓ **Securus has read, understands, and complies.**

4.13 INVOICES AND PAYMENTS:

4.13.1 The Respondent shall submit two (2) legible copies of their detailed invoice before payment(s) can be made. At a minimum, the invoice must provide the following information:

- Company name, address and contact
- County bill-to name and contact information
- Contract Serial Number
- County purchase order number
- Invoice number and date
- Payment terms
- Date of service or delivery
- Quantity
- Contract Item number(s)
- Description of Purchase (services)
- Pricing per unit of service
- Extended price
- Total Amount Due

✓ **Securus has read, understands, and complies.**

As this is a no-cost solution to Maricopa County, there is no need for Securus to present the county with invoices for payment of services.

4.13.2 Problems regarding billing or invoicing shall be directed to the using agency as listed on the Purchase Order

✓ **Securus has read, understands, and complies.**

SCBS will handle all billing and invoicing.

4.13.3 Payment shall be made to the Contractor by Accounts Payable through the Maricopa County Vendor Express Payment Program. This is an Electronic Funds Transfer (EFT) process. After Contract Award the Contractor shall complete the Vendor Registration Form located on the County Department of Finance Vendor Registration Web Site (www.maricopa.gov/finance/vendors).

✓ **Securus has read, understands, and complies.**

4.13.4 EFT payments to the routing and account numbers designated by the Contractor will include the details on the specific invoices that the payment covers. The

Contractor is required to discuss remittance delivery capabilities with their designated financial institution for access to those details.

✓ **Securus has read, understands, and complies.**

4.14 TAX: (SERVICES)

No tax shall be levied against labor. It is the responsibility of the Contractor to determine any and all taxes and include the same in proposal price.

✓ **Securus has read, understands, and complies.**

4.15 TAX: (COMMODITIES)

Tax shall not be levied against labor. Sales/use tax will be determined by County. Tax will not be used in determine low price.

✓ **Securus has read, understands, and complies.**

4.16 DELIVERY:

It shall be the Contractor's responsibility to meet the proposed delivery requirements. Maricopa County reserves the right to obtain services on the open market in the event the Contractor fails to make delivery and any price differential will be charged against the Contractor.

✓ **Securus has read, understands, and complies.**

4.17 STRATEGIC ALLIANCE for VOLUME EXPENDITURES (\$AVE):

The County is a member of the \$AVE cooperative purchasing group. \$AVE includes the State of Arizona, many Phoenix metropolitan area municipalities, and many K-12 unified school districts. Under the \$AVE Cooperative Purchasing Agreement, and with the concurrence of the successful Respondent under this solicitation, a member of \$AVE may access a contract resulting from a solicitation issued by the County. If you do not want to grant such access to a member of \$AVE, please so state in your proposal. In the absence of a statement to the contrary, the County will assume that you do wish to grant access to any contract that may result from this Request for Proposal.

✓ **Securus has read, understands, and complies.**

4.18 INTERGOVERNMENTAL COOPERATIVE PURCHASING AGREEMENTS (ICPA's)

County currently holds ICPA's with numerous governmental entities throughout the State of Arizona. These agreements allow those entities, with the approval of the Contractor, to purchase their requirements under the terms and conditions of the County Contract. Please indicate on Attachment A, your acceptance or rejection regarding such participation of other governmental entities. Your response will not be considered as an evaluation factor in awarding a contract.

✓ **Securus has read, understands, and complies.**

5.0 SPECIAL TERMS & CONDITIONS:

5.1 CONTRACT TERM:

This Request for Proposal is for awarding a firm, fixed revenue contract to cover a five (5) year term.

✓ **Securus has read, understands, and complies.**

5.2 OPTION TO RENEW CONTRACT:

The County may, at its option and with the approval of the Contractor, renew the term of this Contract up to a maximum of five (5) additional years, or other specified length options, (or at the County's sole discretion, extend the contract on a month to month basis for a maximum of six (6) months after expiration). The Contractor shall be notified in writing by the Office of Procurement Services of the County's intention to extend the contract term at least thirty (30) calendar days prior to the expiration of the original contract term.

✓ **Securus has read, understands, and complies.**

5.3 PRICE ADJUSTMENTS:

Any requests for reasonable price adjustments must be submitted sixty (60) days prior to the Contract annual anniversary date. Requests for adjustment in cost of labor and/or materials must be supported by appropriate documentation. If County agrees to the adjusted price terms, County shall issue written approval of the change. The reasonableness of the request will be determined by comparing the request with the (Consumer Price Index) or by performing a market survey.

✓ **Securus has read, understands, and complies.**

5.4 INDEMNIFICATION:

5.4.1 To the fullest extent permitted by law, Contractor shall defend, indemnify, and hold harmless County, its agents, representatives, officers, directors, officials, and employees from and against all claims, damages, losses and expenses,

including, but not limited to, attorney fees, court costs, expert witness fees, and the cost of appellate proceedings, relating to, arising out of, or alleged to have resulted from the negligent acts, errors, omissions, mistakes or malfeasance relating to the performance of this Contract. Contractor's duty to defend, indemnify and hold harmless County, its agents, representatives, officers, directors, officials, and employees shall arise in connection with any claim, damage, loss or expense that is caused by any negligent acts, errors, omissions or mistakes in the performance of this Contract by the Contractor, as well as any person or entity for whose acts, errors, omissions, mistakes or malfeasance Contractor may be legally liable.

✓ **Securus has read, understands, and complies.**

5.4.2 The amount and type of insurance coverage requirements set forth herein will in no way be construed as limiting the scope of the indemnity in this paragraph.

✓ **Securus has read, understands, and complies.**

5.4.3 The scope of this indemnification does not extend to the sole negligence of County.

✓ **Securus has read, understands, and complies.**

5.5 INSURANCE:

5.5.1 Contractor, at Contractor's own expense, shall purchase and maintain the herein stipulated minimum insurance from a company or companies duly licensed by the State of Arizona and possessing a current A.M. Best, Inc. rating of A+. In lieu of State of Arizona licensing, the stipulated insurance may be purchased from a company or companies, which are authorized to do business in the State of Arizona, provided that said insurance companies meet the approval of County. The form of any insurance policies and forms must be acceptable to County.

✓ **Securus has read, understands, and complies.**

Please refer to Appendix C: Certificate of Insurance for a copy of Securus' insurance policy that details coverages required in this section.

5.5.2 All insurance required herein shall be maintained in full force and effect until all work or service required to be performed under the terms of the Contract is satisfactorily completed and formally accepted. Failure to do so may, at the sole discretion of County, constitute a material breach of this Contract.

✓ **Securus has read, understands, and complies.**

5.5.3 Contractor's insurance shall be primary insurance as respects County, and any insurance or self-insurance maintained by County shall not contribute to it.

✓ **Securus has read, understands, and complies.**

5.5.4 Any failure to comply with the claim reporting provisions of the insurance policies or any breach of an insurance policy warranty shall not affect the County's right to coverage afforded under the insurance policies.

✓ **Securus has read, understands, and complies.**

5.5.5 The insurance policies may provide coverage that contains deductibles or self-insured retentions. Such deductible and/or self-insured retentions shall not be applicable with respect to the coverage provided to County under such policies. Contractor shall be solely responsible for the deductible and/or self-insured retention and County, at its option, may require Contractor to secure payment of such deductibles or self-insured retentions by a surety bond or an irrevocable and unconditional letter of credit.

✓ **Securus has read, understands, and complies.**

5.5.6 County reserves the right to request and to receive, within 10 working days, certified copies of any or all of the herein required insurance certificates. County shall not be obligated to review policies and/or endorsements or to advise Contractor of any deficiencies in such policies and endorsements, and such receipt shall not relieve Contractor from, or be deemed a waiver of County's right to insist on strict fulfillment of Contractor's obligations under this Contract.

✓ **Securus has read, understands, and complies.**

5.5.7 The insurance policies required by this Contract, except Workers' Compensation, shall name County, its agents, representatives, officers, directors, officials and employees as Additional Insureds.

✓ **Securus has read, understands, and complies.**

5.5.8 The policies required hereunder, except Workers' Compensation, shall contain a waiver of transfer of rights of recovery (subrogation) against County, its agents,

representatives, officers, directors, officials and employees for any claims arising out of Contractor's work or service.

✓ **Securus has read, understands, and complies.**

5.5.9 Commercial General Liability:

Commercial General Liability insurance and, if necessary, Commercial Umbrella insurance with a limit of not less than \$2,000,000 for each occurrence, \$2,000,000 Products/Completed Operations Aggregate, and \$4,000,000 General Aggregate Limit. The policy shall include coverage for bodily injury, broad form property damage, personal injury, products and completed operations and blanket contractual coverage, and shall not contain any provision which would serve to limit third party action over claims.

There shall be no endorsement or modification of the CGL limiting the scope of coverage for liability arising from explosion, collapse, or underground property damage.

✓ **Securus has read, understands, and complies.**

5.5.10 Automobile Liability:

Commercial/Business Automobile Liability insurance and, if necessary, Commercial Umbrella insurance with a combined single limit for bodily injury and property damage of not less than \$2,000,000 each occurrence with respect to any of the Contractor's owned, hired, and non-owned vehicles assigned to or used in performance of the Contractor's work or services under this Contract.

✓ **Securus has read, understands, and complies.**

5.5.11 Workers' Compensation:

5.5.11.1 Workers' Compensation insurance to cover obligations imposed by federal and state statutes having jurisdiction of Contractor's employees engaged in the performance of the work or services under this Contract; and Employer's Liability insurance of not less than \$1,000,000 for each accident, \$1,000,000 disease for each employee, and \$1,000,000 disease policy limit.

✓ **Securus has read, understands, and complies.**

5.5.11.2 Contractor waives all rights against County and its agents, officers, directors and employees for recovery of damages to the extent these damages are covered by the Workers' Compensation and Employer's

Liability or commercial umbrella liability insurance obtained by Contractor pursuant to this Contract.

✓ **Securus has read, understands, and complies.**

5.5.12 Certificates of Insurance.

5.5.12.1 Prior to commencing work or services under this Contract, Contractor shall have insurance in effect as required by the Contract in the form provided by the County, issued by Contractor's insurer(s), as evidence that policies providing the required coverage, conditions and limits required by this Contract are in full force and effect. Such certificates shall be made available to the County upon ten (10) business days. BY SIGNING THE AGREEMENT PAGE THE CONTRACTOR AGREES TO THIS REQUIREMENT AND FAILURE TO MEET THIS REQUIREMENT WILL RESULT IN CANCELLATION OF CONTRACT.

✓ **Securus has read, understands, and complies.**

5.5.12.1.1 In the event any insurance policy (ies) required by this contract is (are) written on a "claims made" basis, coverage shall extend for two years past completion and acceptance of Contractor's work or services and as evidenced by annual Certificates of Insurance.

✓ **Securus has read, understands, and complies.**

5.5.12.1.2 If a policy does expire during the life of the Contract, a renewal certificate must be sent to County fifteen (15) days prior to the expiration date.

✓ **Securus has read, understands, and complies.**

5.5.13 Cancellation and Expiration Notice.

Insurance required herein shall not be permitted to expire, be canceled, or materially changed without thirty (30) days prior written notice to the County.

✓ **Securus has read, understands, and complies.**

5.6 ACCESS TO AND RETENTION OF RECORDS FOR THE PURPOSE OF AUDIT AND/OR OTHER REVIEW:

- 5.6.1 In accordance with section MCI 371 of the Maricopa County Procurement Code the Contractor agrees to retain all books, records, accounts, statements, reports, files, and other records and back-up documentation relevant to this Contract for six (6) years after final payment or until after the resolution of any audit questions which could be more than six (6) years, whichever is latest. The County, Federal or State auditors and any other persons duly authorized by the Department shall have full access to, and the right to examine, copy and make use of, any and all said materials.

✓ **Securus has read, understands, and complies.**

- 5.6.2 If the Contractor's books, records, accounts, statements, reports, files, and other records and back-up documentation relevant to this Contract are not sufficient to support and document that requested services were provided, the Contractor shall reimburse Maricopa County for the services not so adequately supported and documented.

✓ **Securus has read, understands, and complies.**

5.7 PROCUREMENT CARD ORDERING CAPABILITY:

County may determine to use a procurement card (MasterCard), from time-to-time, to place or make payment for orders under the Contract. Respondents without this capability may be considered non-responsive and not eligible for award consideration.

✓ **Securus has read, understands, and complies.**

5.8 INTERNET ORDERING CAPABILITY:

County intends to use the Internet to communicate and to place orders under this Contract. Respondents without this capability may be considered non-responsive and not eligible for award consideration.

✓ **Securus has read, understands, and complies.**

5.9 ORDERING AUTHORITY.

- 5.9.1 Respondents should understand that any request for purchase of materials or services shall be accompanied by a valid purchase order, issued by Office of Procurement Services, or by a Certified Agency Procurement Aid (CAPA).

✓ **Securus has read, understands, and complies.**

- 5.9.2 Maricopa County departments, cities, other counties, schools and special districts, universities, nonprofit educational and public health institutions may also purchase from under this Contract at their discretion and/or other state and local agencies (Customers) may procure the products under this Contract by the issuance of a purchase order to the Respondent. Purchase orders must cite the Contract number.

✓ **Securus has read, understands, and complies.**

- 5.9.3 Contract award is in accordance with the Maricopa County Procurement Code. All requirements for the competitive award of this Contract have been met. A purchase order for the products is the only document necessary for Customers to purchase and for the Respondent to proceed with delivery of materials available under this Contract.

✓ **Securus has read, understands, and complies.**

- 5.9.4 Any attempt to represent any product not specifically awarded under this Contract is a violation of the Contract. Any such action is subject to the legal and contractual remedies available to the County, inclusive of, but not limited to, Contract cancellation, suspension and/or debarment of the Respondent.

✓ **Securus has read, understands, and complies.**

5.10 TERMINATION FOR CONVENIENCE:

The County reserves the right to terminate the Contract, in whole or in part at any time, when in the best interests of the County without penalty or recourse. Upon receipt of the written notice, the Contractor shall immediately stop all work, as directed in the notice, notify all subcontractors of the effective date of the termination and minimize all further costs to the County. In the event of termination under this paragraph, all documents, data and reports prepared by the Contractor under the Contract shall become the property of and be delivered to the County upon demand. The Contractor shall be entitled to receive just and equitable compensation for work in progress, work completed and materials accepted before the effective date of the termination.

✓ **Securus has read, understands, and complies.**

5.11 TERMINATION FOR DEFAULT:

- 5.11.1 In addition to the rights reserved in the Contract, the County may terminate the Contract in whole or in part due to the failure of the Contractor to comply with any term or condition of the Contract, to acquire and maintain all required insurance policies, bonds, licenses and permits, or to make satisfactory progress in

performing the Contract. The Procurement Officer shall provide written notice of the termination and the reasons for it to the Contractor.

✓ **Securus has read, understands, and complies.**

5.11.2 Upon termination under this paragraph, all goods, materials, documents, data and reports prepared by the Contractor under the Contract shall become the property of and be delivered to the County on demand.

✓ **Securus has read, understands, and complies.**

5.11.3 The County may, upon termination of this Contract, procure, on terms and in the manner that it deems appropriate, materials or services to replace those under this Contract. The Contractor shall be liable to the County for any excess costs incurred by the County in procuring materials or services in substitution for those due from the Contractor.

✓ **Securus has read, understands, and complies.**

5.11.4 The Contractor shall continue to perform, in accordance with the requirements of the Contract, up to the date of termination, as directed in the termination notice.

5.12 TERMINATION BY THE COUNTY:

If the Contractor should be adjudged bankrupt or should make a general assignment for the benefit of its creditors, or if a receiver should be appointed on account of its insolvency, the County may terminate the Contract. If the Contractor should persistently or repeatedly refuse or should fail, except in cases for which extension of time is provided, to provide enough properly skilled workers or proper materials, or persistently disregard laws and ordinances, or not proceed with work or otherwise be guilty of a substantial violation of any provision of this Contract, then the County may terminate the Contract. Prior to termination of the Contract, the County shall give the Contractor fifteen-(15) calendar day's written notice. Upon receipt of such termination notice, the Contractor shall be allowed fifteen (15) calendar days to cure such deficiencies.

✓ **Securus has read, understands, and complies.**

5.13 ADDITIONS/DELETIONS OF SERVICE:

5.13.1 The County reserves the right to add and/or delete materials to a Contract. If a service requirement is deleted, payment to the Contractor will be reduced proportionately, to the amount of service reduced in accordance with the bid price. If additional materials are required from a Contract, prices for such additions will be negotiated between the Contractor and the County.

✓ **Securus has read, understands, and complies.**

5.13.2 The County reserves the right of final approval on proposed staff for all Task Orders. Also, upon request by the County, the Contractor will be required to remove any employees working on County projects and substitute personnel based on the discretion of the County within two business days, unless previously approved by the County.

✓ **Securus has read, understands, and complies.**

5.14 SUBCONTRACTING:

5.14.1 The Contractor may not assign a Contract or Subcontract to another party for performance of the terms and conditions hereof without the written consent of the County. All correspondence authorizing subcontracting must reference the Bid Serial Number and identify the job project.

✓ **Securus has read, understands, and complies.**

5.14.2 The Subcontractor's rate for the job shall not exceed that of the Prime Contractor's rate, as bid in the pricing section, unless the Prime Contractor is willing to absorb any higher rates. The Subcontractor's invoice shall be invoiced directly to the Prime Contractor, who in turn shall pass-through the costs to the County, without mark-up. A copy of the Subcontractor's invoice must accompany the Prime Contractor's invoice.

✓ **Securus has read, understands, and complies.**

5.15 SCHEDULE OF EVENTS:

Request for Proposals Issued: January 24th, 2013

Pre-Proposal Conference: February 11th, 2013

Deadline for written questions is (2) business days after Pre-Proposal Conference. Questions will ***not*** be responded to prior to the Pre-Proposal Conference or after the (2) business day deadline has elapsed. All questions and answers shall be posted to www.bidsync.com under the Q&A's tab for the solicitation and must be received by the end of business, 5:00 PM Arizona time *(Note: The following dates were changed in Addendum 3 and are noted below by strikethrough text with new dates underlined.)*

Proposals Opening Date: ~~March 4th, 2013~~ March 22nd, 2013

Deadline for submission of proposals is 2:00 P.M., Arizona Time, on ~~March 4th~~, 2013 March 22nd, 2013. All proposals must be received before 2:00 P.M., Arizona Time, on the above date at the Maricopa County Office of Procurement Services, 320 West Lincoln Street, Phoenix, Arizona 85003.

Proposed review of Proposals and short list decision: ~~March 15th~~, 2013 April 5th, 2013

Proposed Respondent presentations: (if required) ~~March 25th~~, 2013 April 15th, 2013

Proposed selection and negotiation: ~~April 8th~~, 2013 April 20th, 2013

Proposed Best & Final (if required) ~~April 15nd~~, 2013 May 6th, 2013

Proposed award of Contract: ~~May 1st~~, 2013 May 22nd, 2013

All responses to this Request for Proposal become the property of Maricopa County and (other than pricing) will be held confidential, to the extent permissible by law. The County will not be held accountable if material from proposal responses is obtained without the written consent of the Respondent by parties other than the County.

✓ **Securus has read, understands, and complies.**

5.16 INQUIRIES AND NOTICES:

All inquiries concerning information herein shall be addressed to:

Maricopa County Office of
Procurement Services ATTN:
Contract Administration 320
West Lincoln Street Phoenix,
Arizona 85003-2494

Administrative telephone inquiries shall be addressed to:

Paul Aguilar, Procurement Officer, 602/506-
3248 (aguilarp001@mail.maricopa.gov)

✓ **Securus has read, understands, and complies.**

5.17 INSTRUCTIONS FOR PREPARING AND SUBMITTING PROPOSALS:

Respondents shall provide their proposals in accordance with Section 3.14 as follows:

5.17.1 One (1) original hardcopy of all proposal documents.

5.17.2 One (1) CD or flash drive providing all proposal documents in Word, Excel (Attachment A) and then the entire proposal document in PDF format.

5.17.3 Seven (7) CD's or flash drives providing the entire proposal in PDF format only.

- 5.17.4 Respondents shall address proposals identified with return address, serial number and title in the following manner:

Maricopa County
Office of Procurement Services
320 West Lincoln Street
Phoenix, Arizona 85003-2494

SERIAL 13002 – RFP, WEB-BASED VISITATION/COMMUNICATION KIOSK SYSTEM

- 5.17.5 Proposals shall be signed by an owner, partner or corporate official who has been authorized to make such commitments. All prices shall be held firm for a period of one hundred fifty (150) days after the RFP closing date.

✓ **Securus has read, understands, and complies.**

5.18 EXCEPTIONS TO THE SOLICITATION:

The Respondent shall identify and list all exceptions taken to all sections of 13002-RFP and list these exceptions referencing the section (paragraph) where the exception exists and identify the exceptions and the proposed wording for the Respondent's exception under the heading, "Exception to the PROPOSAL Solicitation, SERIAL 13002-RFP." **Exceptions that surface elsewhere and that do not also appear under the heading, "Exceptions to the PROPOSAL Solicitation, SERIAL 13002-RFP," shall be considered invalid and void and of no contractual significance.**

The County reserves the right to reject, determine the proposal non-responsive, enter into negotiation on any of the Respondent exceptions, or accept them outright.

✓ **Securus has read, understands, and complies.**

Securus notes its exceptions in the section titled "5.20.6 Proposal Exceptions" as instructed in RFP section 5.20 Format and Content.

5.19 GENERAL CONTENT:

- 5.19.1 The Proposal should be specific and complete in every detail. It should be practical and provide a straightforward, concise delineation of capabilities to satisfactorily perform the Contract being sought.

✓ **Securus has read, understands, and complies.**

- 5.19.2 The Respondent should not necessarily limit the proposal to the performance of the services in accordance with this Request for Proposal but should outline any additional services and their costs if the Respondent deems them necessary to accomplish the program.

✓ **Securus has read, understands, and complies.**

5.20 FORMAT AND CONTENT:

To aid in the evaluation, it is desired that all proposals follow the same general format. The proposal hardcopy must be submitted in binders and have sections tabbed as below: (Responses are limited to 200 pages, single sided, 10 point font type).

5.20.1 Table of Contents

5.20.2 Letter of Transmittal (Exhibit 2)

5.20.3 Executive Summary - This section shall contain an outline of the general approach utilized in the proposal.

5.20.4 Proposal - This section should contain a statement of all of the programs and services proposed, including conclusions and generalized recommendations. Proposals should be all-inclusive, detailing respondent's best offer.

5.20.5 Qualifications - This section shall describe the respondent's ability and experience related to the programs and services proposed. All project personnel, as applicable, shall be listed including a description of assignments and responsibilities, a resume of professional experience, an estimate of the time each would devote to this program, and other pertinent information.

5.20.6 Proposal exceptions

5.20.7 Other data

5.20.8 Attachment A (Pricing)

5.20.9 Attachment B (Agreement Page)

5.20.10 Attachment C (References)

5.20.11 Attachment D (Questionnaire)

5.20.12 Exhibit 3, Sole Proprietor Waiver (If applicable)

✓ **Securus has read, understands, and complies.**

5.21 EVALUATION OF PROPOSAL - SELECTION FACTORS:

A Proposal Evaluation Committee shall be appointed, chaired by the Procurement Officer to evaluate each Proposal. At the County's option, Respondents may be invited to make presentations to the Evaluation Committee. Best and Final Offers and/or Negotiations may be conducted, as needed, with the highest rated Respondent(s). Proposals will be evaluated on the following criteria which are listed descending order of importance.

5.21.1 Experience and Qualifications of firm

5.21.2 Proposals meets specifications of solicitation

5.21.3 Proposed revenue plan

✓ **Securus has read, understands, and complies.**

5.22 CERTIFICATION REGARDING DEBARMENT AND SUSPENSION:

5.22.1 The undersigned (authorized official signing for the Contractor) certifies to the best of his or her knowledge and belief, that the Contractor, defined as the primary participant in accordance with 45 CFR Part 76, and its principals:

5.22.1.1 are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal Department or agency;

✓ **Securus has read, understands, and complies.**

5.22.1.2 have not within 3-year period preceding this Contract been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

✓ **Securus has read, understands, and complies.**

5.22.1.3 are not presently indicted or otherwise criminally or civilly charged by a government entity (Federal, State or local) with commission of any of the offenses enumerated in paragraph (2) of this certification; and

✓ **Securus has read, understands, and complies.**

5.22.1.4 have not within a 3-year period preceding this Contract had one or more public transaction (Federal, State or local) terminated for cause of default.

5.22.2 Should the Contractor not be able to provide this certification, an explanation as to why should be attached to the Contact.

✓ **Securus has read, understands, and complies.**

5.22.3 The Contractor agrees to include, without modification, this clause in all lower tier covered transactions (i.e. transactions with subcontractors) and in all solicitations for lower tier covered transactions related to this Contract.

✓ **Securus has read, understands, and complies.**

5.23 VERIFICATION REGARDING COMPLIANCE WITH ARIZONA REVISED STATUTES §41-4401 AND FEDERAL IMMIGRATION LAWS AND REGULATIONS:

5.23.1 By entering into the Contract, the Contractor warrants compliance with the Immigration and Nationality Act (INA using e-verify) and all other federal immigration laws and regulations related to the immigration status of its employees and A.R.S. §23-214(A). The contractor shall obtain statements from its subcontractors certifying compliance and shall furnish the statements to the Procurement Officer upon request. These warranties shall remain in effect through the term of the Contract. The Contractor and its subcontractors shall also maintain Employment Eligibility Verification forms (I-9) as required by the Immigration Reform and Control Act of 1986, as amended from time to time, for all employees performing work under the Contract and verify employee compliance using the E-verify system and shall keep a record of the verification for the duration of the employee's employment or at least three years, whichever is longer. I-9 forms are available for download at USCIS.GOV.

✓ **Securus has read, understands, and complies.**

5.23.2 The County retains the legal right to inspect contractor and subcontractor employee documents performing work under this Contract to verify compliance with paragraph 5.23.1 of this Section. Contractor and subcontractor shall be given reasonable notice of the County's intent to inspect and shall make the documents available at the time and date specified. Should the County suspect or find that the Contractor or any of its subcontractors are not in compliance, the County will consider this a material breach of the contract and may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

✓ **Securus has read, understands, and complies.**

5.24 VERIFICATION REGARDING COMPLIANCE WITH ARIZONA REVISED STATUTES §§35-391.06 AND 35-393.06 BUSINESS RELATIONS WITH SUDAN AND IRAN:

5.24.1 By entering into the Contract, the Contractor certifies it does not have scrutinized business operations in Sudan or Iran. The contractor shall obtain statements from its subcontractors certifying compliance and shall furnish the statements to the Procurement Officer upon request. These warranties shall remain in effect through the term of the Contract.

✓ **Securus has read, understands, and complies.**

5.24.2 The County may request verification of compliance for any contractor or subcontractor performing work under the Contract. Should the County suspect or find that the Contractor or any of its subcontractors are not in compliance, the County may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

✓ **Securus has read, understands, and complies.**

5.25 CONTRACTOR LICENSE REQUIREMENT:

5.25.1 The Respondent shall procure all permits, insurance, licenses and pay the charges and fees necessary and incidental to the lawful conduct of his/her business, and as necessary complete any required certification requirements, required by any and all governmental or non-governmental entities as mandated to maintain compliance with and in good standing for all permits and/or licenses. The Respondent shall keep fully informed of existing and future trade or industry requirements, Federal, State and Local laws, ordinances, and regulations which in any manner affect the fulfillment of a Contract and shall comply with the same. Contractor shall immediately notify both Office of Procurement Services and the using agency of any and all changes concerning permits, insurance or licenses.

✓ **Securus has read, understands, and complies.**

5.25.2 Respondents furnishing finished products, materials or articles of merchandise that will require installation or attachment as part of the Contract, shall possess any licenses required. A Respondent is not relieved of its obligation to possess the required licenses by subcontracting of the labor portion of the Contract. Respondents are advised to contact the Arizona Registrar of Contractors, Chief of Licensing, at (602) 542-1502 to ascertain licensing requirements for a particular contract. Respondents shall identify which license(s), if any, the Registrar of Contractors requires for performance of the Contract.

✓ **Securus has read, understands, and complies.**

5.26 INFLUENCE

As prescribed in MC1-1202 of the Maricopa County Procurement Code, any effort to influence an employee or agent to breach the Maricopa County Ethical Code of Conduct or any ethical conduct, may be grounds for Disbarment or Suspension under MC1-902. An attempt to influence includes, but is not limited to:

5.26.1 A Person offering or providing a gratuity, gift, tip, present, donation, money, entertainment or educational passes or tickets, or any type valuable contribution or subsidy, ;

✓ **Securus has read, understands, and complies.**

5.26.2 That is offered or given with the intent to influence a decision, obtain a contract, garner favorable treatment, or gain favorable consideration of any kind.

If a Person attempts to influence any employee or agent of Maricopa County, the Chief Procurement Officer, or his designee, reserves the right to seek any remedy provided by the Maricopa County Procurement Code, any remedy in equity or in the law, or any remedy provided by this contract.

✓ **Securus has read, understands, and complies.**

5.27 POST AWARD MEETING:

The successful Respondent shall be required to attend a post-award meeting with the Using Agency to discuss the terms and conditions of the Contract. This meeting will be coordinated by the Procurement Officer of the Contract.

✓ **Securus has read, understands, and complies.**

5.20.5 Qualifications

This section shall describe the respondent's ability and experience related to the programs and services proposed. All project personnel, as applicable, shall be listed including a description of assignments and responsibilities, a resume of professional experience, an estimate of the time each would devote to this program, and other pertinent information.

✓ **Securus has read, understands, and complies.**

SVV fulfills the requirements of this RFP is an integrated Web-based, real-time, corrections based communication system. SVV is a combination of state-of-the-art video conferencing technology, browser-based network control and scheduling, enterprise-level computing and storage, with the most sophisticated digital recording and monitoring on the market today. By offering a zero cost solution which allows for visitors to visit from home/remotely, it will reduce labor, and automate systems.

SVV is a 100 percent Web-based video visitation platform and integrated inmate kiosk solution specifically designed for correctional facilities.

SVV will enable Maricopa County to conduct visitations safely, securely, and with fewer burdens on facility staff. This advanced solution provides multiple benefits, including:

- Enhanced facility security by reducing the possibility of inmate confrontation
- Reduction in inmate and visitor movement through a facility
- Improved inmate ability to communicate with legal representation, bail-bond facilities, family, and any other persons authorized by Maricopa County Jail administration
- Reduction in contraband infiltration
- Increased security for visitors
- Increased inmate and visitor morale with increased opportunities to visit
- Reduced resources needed to escort inmates and visitors to visiting areas
- New revenue stream for the facility through paid visitation sessions

The SVV solution is a centralized system that allows for automatic technology and feature upgrades. After the video visitation system has been implemented, it is easy for Securus to enable new features and modules by activating the feature in the centralized system.

At-home or remote visitation sessions allow friends and family, bail bondsmen, probation officers, and attorneys to securely communicate with inmates from outside the facility via a broadband Internet connection.

Remote visitors access Securus Video Visitation through the www.securustech.net Web site. The visitor selects the facility and inmate they would like to visit. The visitor is able to do the following:

- Create, edit, and/or delete scheduled video sessions with inmates
- Pay for the scheduled session with a credit or debit card
- Visit with inmates (no officer intervention required)

Remote users will need to use a personal computer or laptop with a built-in or external USB Web camera, a microphone and speakers, or a headset.

Project Personnel

Securus anticipates the following personnel will support Maricopa County either during the implementation of SVV or on an ongoing basis:

- **Darrin Hays: Account Manager.** Darrin is assigned as Maricopa County's single point of contact for all needs you may have that Securus can meet. Darrin's focus is to ensure that the system is meeting your needs. He also will help train Maricopa County staff on the system and act as your advocate within Securus. Darrin will serve Maricopa County on an ongoing basis.
- **Ron Davis: Sales Vice President.** In addition to Darrin's role as Maricopa County's advocate, Ron provide executive oversight, ensuring that your Securus is providing services to your expectations. Ron will serve Maricopa County on an ongoing basis.
- **Greg Nicholson: Sales Engineer.** Greg applies his technical expertise and works with Darrin and Ron to identify products and services that can further benefit Maricopa County. Greg also will help train Maricopa County personnel and advise you in the most effective and efficient uses of our systems and services. Greg will serve Maricopa County on an ongoing basis.
- **Jamie Mungo: Project Manager.** Jamie will help plan and lead the implementation of SVV at Maricopa County. Jamie has led and participated in numerous implementations. She will be involved with the project until the implementation is approved and accepted by Maricopa County and service turned over to the account team.
- **David Beeley: Field Service Specialist.** David, our highest grade of Field Service Technician, will support the implementation of SVV at Maricopa County.
- **Josh Farrar: Field Service Specialist.** Josh, also our highest grade of Field Service Technician, will support the implementation of SVV at Maricopa County.
- **Frank Gonzalez: Field Service Technician.** Frank will support the implementation of SVV at Maricopa County and also provide ongoing technical support of the system.
- **Lori Simmons: Field Service Technician.** Lori will support the implementation of SVV at Maricopa County and also provide ongoing technical support of the system.
- **John Jacoby: Field Service Manager.** John will provide management oversight support both the implementation and ongoing operations.

- **On-Site Administrators:** Upon selection as your VVS provider, Securus will hire and train—or transfer to Maricopa County—three on-site administrators. Because you will be working so closely with them, Maricopa County will have approval authority over who fill these positions.

Resumes for the above Securus staff are in Appendix D: Resumes in the Other Data section.

5.20.6 Proposal Exceptions

The Respondent shall identify and list all exceptions taken to all sections of 13002-RFP and list these exceptions referencing the section (paragraph) where the exception exists and identify the exceptions and the proposed wording for the Respondent's exception under the heading, "Exception to the PROPOSAL Solicitation, SERIAL 13002-RFP." Exceptions that surface elsewhere and that do not also appear under the heading, "Exceptions to the PROPOSAL Solicitation, SERIAL 13002-RFP," shall be considered invalid and void and of no contractual significance.

The County reserves the right to reject, determine the proposal non-responsive, enter into negotiation on any of the Respondent exceptions, or accept them outright.

✓ **Securus has read, understands, and complies.**

Securus takes three exceptions to the requirements in this RFP. We include the requirement and our responses below.

- 2.5.18 The system shall detect when extra people or voices are present and a notation shall be included in the video detail record of the attempt.

✓ **Securus has read, understands, and does not comply.**

Like all video visitation systems, Securus' SVV does not currently have the ability to detect extra people or voices during the Video Visitation Session. However, Securus is experienced in such technologies and does have the ability to identify registered voices using Voice Biometrics in its Continuous Voice Verification (CVV) product for the Inmate Telephone System. As users of Securus' Inmate Telephone System (SCP), Securus customers avail themselves to the most cutting edge and technologically sophisticated information systems in the industry. These systems will integrate and share information with each other to identify targeted leads, such as our THREADS™ Product.

- 4.8.9 Inmate Tank Order Reports- The contractor shall list any and all reports available and be able to differentiate between requests (i.e. programs, religion, library, ILS). Include an example of each report.

✓ **Securus has read, understands, and does not comply.**

Maricopa County can use SVV's sample report, displayed earlier in this section, to filter details and show different visitation information or request details by inmate.

- 4.8.10 Disciplinary Action Reports- The contractor shall list any and all reports available and include an example of each report.

✓ **Securus has read, understands, and does not comply.**

Securus prides itself on being a partner to our customers and providing high-quality services that meet their needs. We look to improve our services and products based on customer demand, and as a flagship account (should we be selected to provide Maricopa County's video visitation services) we would work with you to fully understand your needs and enhance SVV to create such reports.

5.20.7 Other Data

Securus has several complementary technologies that can supplement SVV and enhance the video visitation experience for inmates and their friends and families as well as provide additional capabilities for Maricopa County, such as the following:

- THREADS™
- TouchPay payment kiosks—more points of payment
- Secure Instant Mail

In addition to the above, Securus includes the following appendices, which further explain our features and capabilities:

- Appendix A: Preliminary Implementation Schedule
- Appendix B: Securus Test and Acceptance Documents and Checklists
- Appendix C: Certificate of Insurance
- Appendix D: Resumes
- Appendix E: Arizona Business Certificates

Threads™

As an option, Securus can provide Maricopa County with our new, powerful investigative software called THREADS™, exclusive to Securus and not available from any other provider.

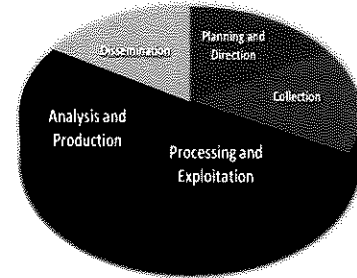
"Major intelligence failures are usually caused by failures of analysis, not failures of collection."

- Richard Heuer Jr., CIA Analyst and Author of *Psychology of Intelligence Analysis*

Securus understands the lifecycle of intelligence and investigating communications data and the challenges investigators, detectives, and corrections facility staff face in both time and resources, such as the following:

- Pulling reports

- Exporting information
- Sending information to someone else
- Contacting other facilities for information
- Combining all the information together
- Receiving information in many different formats
- The daunting task of identifying suspicious behavior in the information provided to uncover focused leads



Even when key information is gathered, investigators have to determine where all of the data will go as well as the time consuming method of analysis.

- What if you had a 24x7 analyst that you didn't have to provide a salary or benefits to?
- How much time and money would be saved?
- What if you had a sense of liability protection knowing access to the data is controlled, logged, tracked, and available to only authorized users?

The Securus THREADS product provides the means to answer these questions. The unique algorithms used within THREADS were designed by real investigators with many years of experience analyzing communications data and training other investigative units on how to analyze data.

Threads Designers

Robert Lottero and Bryan Shouldice were directly involved in designing how THREADS analyzes data. Mr. Lottero is a top expert in telephonic investigative analysis. He leads a group that currently supports the U.S. Department of State, Diplomatic Security Service (DSS) as a communications intelligence analyst.

Mr. Lottero has been involved in criminal investigations, counter-terrorism investigations, and counter-intelligence operations for almost 30 years, both as a contract analyst and as a sworn law enforcement officer. He has provided investigative support to Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Immigration and Naturalization Service (INS), U.S. Customs, New York Police Department (NYPD) Mr. Lottero writes a monthly article for the FBI detailing the latest communication and intelligence techniques that he has developed in his investigative work.

Bryan Shouldice is a 30-year veteran of law enforcement with proven expertise in major case management, intelligence analysis, and international experience in software development and implementation. As a member of the Royal Canadian Mounted Police, Mr. Shouldice conducted major case investigations into all types of criminal activities.

He served as the Executive Case Manager and Intelligence Section Head within the Coordinated Law Enforcement Unit of British Columbia. Mr. Shouldice currently works as an investigative consultant on high-profile cases in the Vancouver Police department.

Managing Investigative Data

Securus understands that during the course of an investigation, the law enforcement community is inundated with data. Data is coming from different sources in different formats with numerous potential leads that can be followed. Each lead potentially creates many more leads to be followed.

We understand investigators are quickly overwhelmed with the amount of information they must analyze as well as the time and resources required to manage, retrieve, and analyze the data to identify those leads that are most likely to uncover important information.

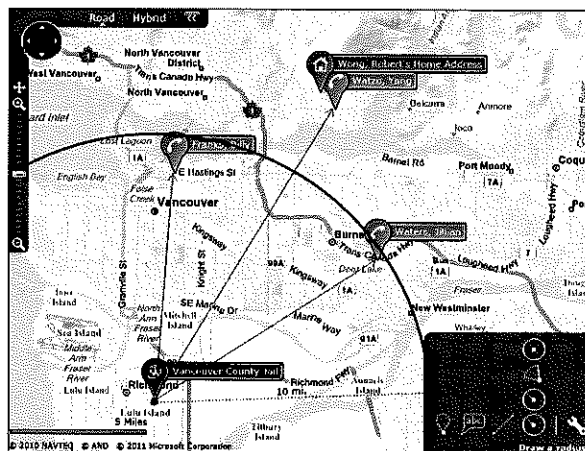
Sources of Information

Corrections Data	External Data
<ul style="list-style-type: none"> Inmate call records Inmate personal information (such as name, account number, PIN, DOB, and SSN) Who the inmate is allowed to call versus who is actually called Called party billing name and address information Public phone records 	<ul style="list-style-type: none"> Confiscated cell phones (such as calls, text messages, emails, videos, and contacts) Corrections facility information in proximity to calling behaviors Events and places of interest Mail Lexus Nexus SS7 information

All corrections data (such as call records, phone numbers, billing name and address) is automatically and fully integrated with THREADS the moment THREADS is enabled. All other sources of data are imported into THREADS and analyzed together to automatically build an investigation.

For example, THREADS will uncover calling patterns that lead to a high probability an inmate has a cell phone. That cell phone is confiscated and the information pulled from it using a Cellebrite UFED device or similar tool. This information is uploaded into THREADS, and all that valuable data is analyzed along with the corrections communication data to uncover an inmate's plot to escape or run an organized crime syndicate from inside the facility.

After determining a suspect on the outside of the facility is involved and mapping out the address, the investigator acquires the public phone records and imports that information into THREADS, which is again analyzed with all the other gathered information. This all takes place in one location, with



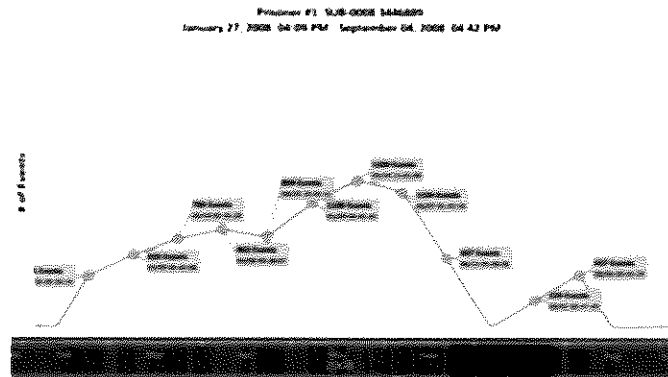
one tool, and is completely integrated with inmate data.

Securus' SCP is the most widely used platform in the industry, with approximately 1,700 facilities installed, more than 850,000 inmates served, literally petabytes of intelligence data, and in excess of 1 million calls processed per day. This valuable data is integrated directly into THREADS and could be available at Maricopa County's fingertips.

Powerful, Accurate, Easy to Use

THREADS is a powerful, accurate, easy-to-use, intuitive tool that will automatically analyze investigative data such as inmate communication records, public phone records, and data from confiscated cell phones to automatically generate focused leads for investigators. Leads can include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple inmates, their correlation to called parties, and much more.

Additionally, this powerful software provides dayroom-based analysis that discovers leads irrespective of the PIN being used by the inmate and common contact reporting showing inmates who are facilitating communications between different areas of the institution. Maricopa County investigative staff can easily uncover patterns of fraternization between inmates and correctional officers, discover common contacts between inmates and called parties, and customize the information and reporting to filter out irrelevant calls such as to girlfriends or legal counsel from analysis.



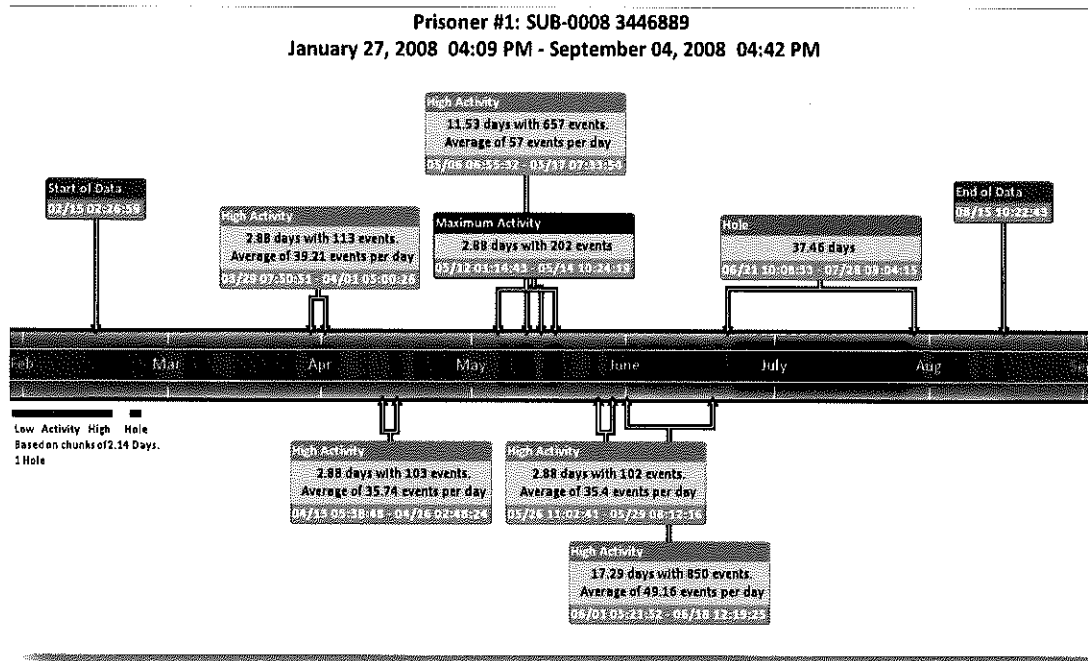
THREADS will detect criminal organizations being run from within jail, detect three-way calling patterns when multiple inmates are talking to one called party at the same time, find associations of multiple called parties based on who is calling them, and identify inmates who possibly have a cell phone based on calling patterns. For instance, if an inmate makes six calls per day, every day, but then all of a sudden doesn't make any for a week, it is possible they have another way to communicate, such as a cell phone.

Graphic Representation

All information is presented graphically as well as textually such as the example presented in the following figure.

Activity and Hole Detection

Proprietary and Confidential



Timeline charts and graphical analysis make it easy to show periods of high-intensity calling and other calling patterns on a graphical and interactive timeline. This technology identifies the inmate even if the calls are masked by another inmate's PIN and eliminates the human intervention by receiving actionable intelligence at the push of a button. Additionally, THREADS allows you to set up automated notifications, which will email an investigator when information is found.

THREADS analyzes data for investigators and provides interactive visualization tools to produce easy-to-understand analytical reports, charts, interactive graphs, maps, and builds a case and presentation view that can be used as evidence in a criminal trial.

Investigative Benefits for Maricopa County

- Cell phone forensics analysis
- Identify accomplices
- Inmates contact people on the outside indirectly, identify who they are "really" contacting
- Identify linkages
- Identify an inmate's inner circle
- Identify associated gang members
- Identify an inmate's communications within jail

- Find unique patterns in communications data
- Follow the money analysis through funding via TouchPay kiosks
- Combine all the data into a single system to analyze
- Harvest all of this information with enhanced reporting tools

Securus' THREADS is an exclusive investigative technology that no other provider can offer to the correctional industry. THREADS will be available as an optional product and empowers Maricopa County with the latest in investigative technology and one of the most powerful investigative tools in the intelligence community.

Not all investigative capabilities are the same across the industry. Securus is the only company that can offer the THREADS analytical software. THREADS is currently used by the United States Border Patrol, the Department of State, the Department of Defense Cyber Crime Center, the United States Drug Enforcement Center, the Department of Homeland Security, and the U.S. Army—THREADS can be fully integrated into the MCSO's suite of investigative systems.

TouchPay Kiosks—Expanded Capabilities

Maricopa County Jail is already familiar with the advantages offered by TouchPay's kiosks, having them currently installed at your facilities. Where Securus can expand your capabilities with the kiosks—we have a long-standing relationship with TouchPay, who is a preferred partner of ours and we frequently work together to serve corrections facilities across the country—is that they can be used to make payments and schedule visitation sessions from any TouchPay kiosk in the state. The system also can be used by investigators to follow the money trail of where and how sessions are paid for.

We currently are engaged with TouchPay in a bid to the Arizona Department of Corrections (ADC)—where Securus provides inmate telephone services—to additionally provide electronic funds transfers (EFTs) across the state. Should we realize the success we anticipate with this bid, Securus and TouchPay will be uniquely positioned to enable any TouchPay kiosk in the state of Arizona to become a point of sale device to pay for and schedule video visitation sessions at Maricopa County.

By leveraging ours and TouchPay's capabilities, we can integrate our EFT payment network with existing County payment networks, greatly expanding the area of coverage where your inmates' friends and family members can schedule and pay for video visitation sessions.

This unique use of our combined networks will allow us to use our existing County payment network, including the kiosk infrastructure for ADC payments, and combine the data with investigative information on deposit transactions between inmates at other corrections institutions. Upon approval and agreement by all parties, the information associated with these transactions could be used to provide additional investigative data, and when fully integrated into our proposed THREADS investigative tool can provide MCSO investigators with important information on where money is going and from whom it is received.

When combined into THREADS with information from other sources, the MCSO will have a more comprehensive view of many more transactions than ever previously available to investigators.

Secure Instant Mail

Traditionally, facilities provide inmate communications through the telephone and through U.S. Mail. Understanding this, Securus has developed a solution to automate facilities' mail processes and make them safer, more secure, less labor intensive, more visible, more investigative, and even profitable.

Secure Instant Mail enables friends and family members to establish a prepaid email account with Securus to securely send and receive email messages to inmates. These prepaid email transactions **are commissionable, adding an incremental source of revenue to Maricopa County**. Secure Instant Mail was designed to take facilities:

From...	To...
A manual mail process	✓ An automated email process
No revenue related to inmate mail	✓ Increased facility revenue through emails
Limited investigative capabilities	✓ Archived, searchable email database
Potential mailed contraband risks	✓ No mailed contraband physically possible
Labor intensive mail security	✓ Increased security through automation
Limited visibility of inmate mail traffic	✓ Interactive email activity dashboard
Facility staff dedicated to a mail room	✓ Anytime, anywhere email review and approval process from laptops or even smart phones
Standard sort and deliver mail method	✓ Flexible mail options designed to work with facilities' unique needs

Secure Instant Mail also considers the communication needs of inmates' friend and family members in Maricopa County communities, enabling them to:

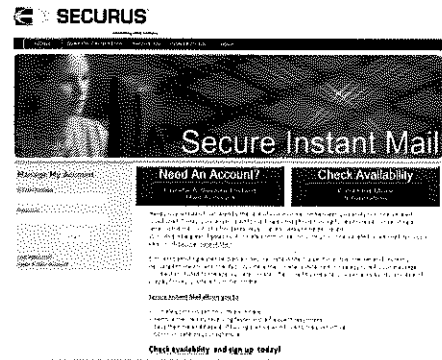
- Access a simple email interface, designed to look and feel like other public email clients.
- Initiate the communication with the inmate to send and receive emails and even pictures—*anytime, anywhere*.
- Gain peace of mind, knowing the inmate received the mail by viewing approved email delivery receipts.
- Communicate more frequently without the need of stamps, envelopes, and on their schedule.

How It Works

Secure Instant Mail is similar to standard email, but built for the corrections environment, meaning it was designed to be flexible, secure, efficient —and profitable.

7. Account Setup and Sending Email

The inmate's friend or family member sets up a Secure Instant Mail account by going to www.securustech.net. Using the Secure Instant Mail website, they can select the facility and inmate receiving the email, compose the email, select messaging options, pay for the email and send the email. Messaging options include requesting approval notifications, prepaying for inmate responses, and even uploading pictures. The email is then processed through the system for the facility's approval before it is sent to the inmate.

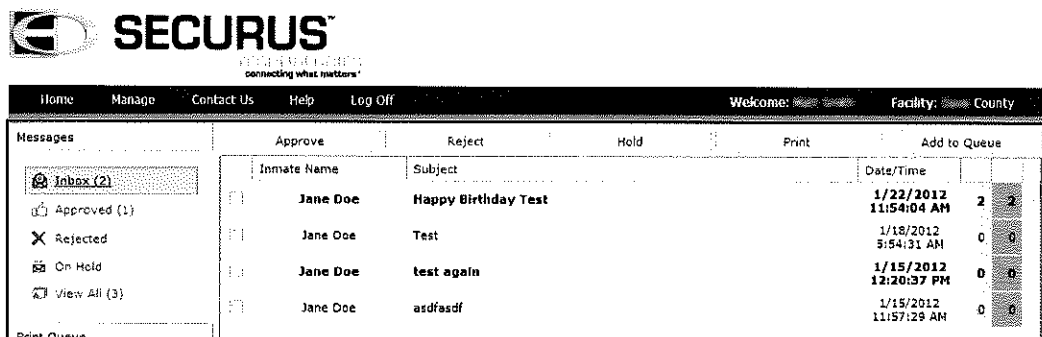


8. Facility Approval

Authorized facility staff logs into the facility's Secure Instant Mail website with a secure user name and password to manage inmate emails. Staff can review, approve, and reject emails and pictures. This process is simplified through a customizable **automatic word search engine**, which flags illicit and potentially illicit words in the emails.

The following figure illustrates the system's capability to flag pending emails that contain word warnings. Their critical relevance is indicated as "red" or "yellow." The facility staff can easily point and click for approval or rejection from any approved PC at anytime, anywhere.

Secure Instant Mail Inbox with Red and Yellow Warning Word Indicator *Proprietary and Confidential*



Once the email is approved, it is archived and can be distributed to the inmate. If the friend or family member has selected to be notified, they would receive an automatic reply email at this time, confirming the approval.

9. Delivery to the Inmate

Maricopa County inmates will receive the email through optional methods including print format and by accessing a Securus Video Visitation kiosk (if available in the facility). Inmates may reply to their email through kiosks or by submitting their written response to facility staff to be approved and scanned into the system to be sent via email to the friend or family member.

Improving Maricopa County Operations through Automation and Innovation

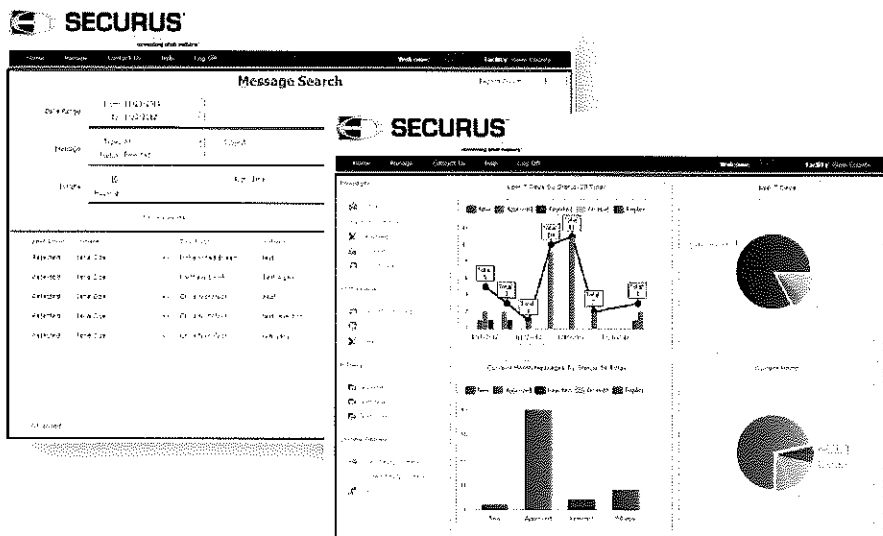
Secure Instant Mail was not only designed to provide Maricopa County with additional revenue, but also to improve mail room operations security and efficiency. This is accomplished through fully integrated technology that places all automated tools needed to create, approve, send, and receive, and respond to email in the hands of the users.

Secure Instant Mail...

- Eliminates the need to open, analyze, sort, translate, or x-ray mail.
- Reduces contraband, improving the safety of Maricopa County officers as well as inmates.
- Speeds up the emails approval process through integrated word search engine with a built-in, editable dictionary.
- Enhances investigations by archiving each email in a secure centralized database. Through the Secure Instant Mail website, investigators can search for emails by inmate, sender, date range, keyword, and much more.
- Provides an interactive dashboard of email traffic by type, status, and date—giving administrators a complete email management tool right at their fingertips.

Secure Instant Mail Message Search and Interactive Dashboard

Proprietary and Confidential



5.20.8 Attachment A (Pricing)

SERIAL 13002 - RFP

NIGP CODE: 83834

COMPANY NAME:

Securus Technologies

DOING BUSINESS AS (DBA) NAME:

Securus Technologies

MAILING ADDRESS:

14651 Dallas Parkway, Suite 600

Dallas, TX 75254

REMIT TO ADDRESS:

Same

TELEPHONE NUMBER:

972-277-0300

FACSIMILE NUMBER:

972-277-0514

WEB SITE:

www.securustech.net

REPRESENTATIVE NAME:

Darrin Hays

REPRESENTATIVE PHONE NUMBER:

480-717-8790

REPRESENTATIVE E-MAIL:

dhays@securustech.net

YES	NO	REBATE
-----	----	--------

WILL ALLOW OTHER GOVERNMENTAL ENTITIES TO PURCHASE FROM THIS CONTRACT:

X []

WILL ACCEPT PROCUREMENT CARD FOR PAYMENT:

X []

FUEL COMPRISES (if section for fuel price adjustment is located in the solicitation document)

0 % OF TOTAL BID AMOUNT

PAYMENT TERMS: RESPONDENT IS REQUIRED TO PICK ONE OF THE FOLLOWING.

PAYMENT TERMS WILL BE CONSIDERED IN DETERMINING LOW BID. FAILURE TO CHOOSE PAYMENT TERMS WILL RESULT IN A DEFAULT TO NET 30 DAYS.

[] NET 10 DAYS

[] NET 45 DAYS

[] 1% 10 DAYS NET 30 DAYS

[] NET 15 DAYS

[] NET 60 DAYS

[] 2% 30 DAYS NET 31 DAYS

[] NET 20 DAYS

[] NET 90 DAYS

[] 1% 30 DAYS NET 31 DAYS

[X] NET 30 DAYS

[] 2% 10 DAYS NET 30 DAYS

[] 5% 30 DAYS NET 31 DAYS

1.0 PROFIT SHARING:

1.1 Please provide the rate you charge visitors for one (1) minute of visitation for web usage:

\$0.6475 based on \$12.95 for a 20

1.2 Please provide a anticipated first payment to MCSO post award and implementation:

After system cost paid through

1.3 Please provide your proposed percentage of profit sharing:

25% for average of one visit pe
27% for average of 1.2 visits pe
29% for average of 1.4 visits pe

ADDITIONAL PRICING

Hourly rates for "out of scope" project personnel

Title	Project Position	Hourly Fee
N/A		

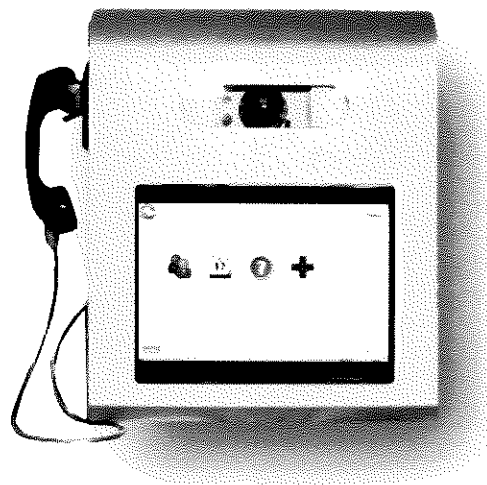
Catalog List Less Percentage Off Discount **	N/A
--	-----

** For items not specifically listed on contract

A Video Visitation Solution for Maricopa County

Securus is excited to provide the Maricopa County Sheriff's Office with a state-of-the-art Securus Video Visitation system, enabling you to conduct visitation sessions safely, securely, and with fewer burdens on facility staff. This advanced solution will provide Maricopa County with multiple benefits, including:

- Enhanced facility security by reducing the possibility of inmate confrontations
- Enhanced facility operations capabilities
- Improved ability of inmates to communicate with legal representation, bail-bond, family, and any other persons authorized by MCSO and facility administration
- Reduced contraband infiltration
- Reduced inmate and visitor movement through your facilities
- Increased security for visitors
- Increased inmate and visitor morale with increased opportunities to visit
- Reduced personnel and man-hours needed to escort inmates and visitors to visiting areas
- Reduction in paper costs and labor by offering an electronic "Forms-Based" solution for Inmate Communications with staff, friends, and family



The Securus Video Visitation solution is a centralized system that allows automatic technology and feature upgrades to ensure your system is always future proof. After the system has been implemented, it is easy for Securus to enable new features and modules by activating the feature in the centralized system—system updates are faster, more efficient, and less intrusive than having to have technicians on site to effect updates.

Our video visitation service provides Securus clients the very best in video visitation without the burden and costs of purchasing and managing the system. We maintain the video visitation system 24 hours a day, 7 days a week, and 365 days a year. The County benefits from a quality of service that is fast, accessible, and secure.

Financial Proposal for Maricopa County

Securus will provide the following at no cost to Maricopa County:

- 343 video visitation terminals (includes visitation centers and inmate terminals)
- Wiring of your facilities with CAT6E cable via conduit
- All electrical cabling to each terminal
- Software application setup – including JMS import mapping

5.20.8 Attachment A (Pricing)

- Video session recording storage – 90 days
- Video visitation software licensing fees
- On-site training on use of the visitation system
- Data network for video visitation traffic

Terms

The video agreement will be for a period of five years, followed with one five-year renewable extension.

Securus will provide the Cat6E cabling, required electrical to each terminal, the Inmate and Visitor Center visitation terminals, Internet bandwidth required, and ongoing support at no charge to Maricopa County.

At-home and remote visitors will be able to schedule either a 20-minute visit for \$12.95 or a 40-minute visit for \$25.90 plus any applicable taxes, fees, and surcharges. There is no charge for on-site visits in the Visitation Center. Professional visits can be configured to 30-minute and 60-minute sessions, if necessary.

Commissions

	1.0 Visits Per Month	1.4 Visits Per Month	1.8 Visits Per Month	2.0 Visits per Month
Cost Per 20-minute Video Session	\$12.95	\$12.95	\$12.95	\$12.95
Average Daily Population	10,800	10,800	10,800	10,800
Commissions	25% upon system payoff	29% upon system payoff	33% upon system payoff	35% upon system payoff
Monthly County Commissions (after system payoff)	\$ 34,965	\$56,783	\$83,077	\$97,902
Annual County Commissions	\$419,580	\$681,398	\$996,922	\$1,174,824

5.20.9 Attachment B (Agreement Page)

AGREEMENT

Respondent hereby certifies that Respondent has read, understands and agrees that acceptance by Maricopa County of the Respondent's Offer will create a binding Contract. Respondent agrees to fully comply with all terms and conditions as set forth in the Maricopa County Procurement Code, and amendments thereto, together with the specifications and other documentary forms herewith made a part of this specific procurement

BY SIGNING THIS PAGE THE SUBMITTING RESPONDENT CERTIFIES THAT RESPONDENT HAS REVIEWED THE ADMINISTRATIVE INFORMATION AND DRAFT RFP CONTRACT'S TERMS AND CONDITIONS LOCATED AT <http://www.maricopa.gov/materials>. AND AGREE TO BE CONTRACTUALLY BOUND TO THEM.

☐ Small Business Enterprise (SBE)

Securus Technologies, Inc.

RESPONDENT (FIRM) SUBMITTING PROPOSAL

75-2722144

FEDERAL TAX ID NUMBER

19-285-8954

DUNS #

Robert E. Pickens, Chief Operating Officer

PRINTED NAME AND TITLE

AUTHORIZED SIGNATURE

15651 Dallas Parkway, Suite 600

ADDRESS

(962) 277-0300 / (972) 277-0514

TELEPHONE

FAX #

Dallas TX 74254

CITY STATE ZIP

February 26, 2013

DATE

www.securustech.net

WEB SITE

bpickens@securustech.net

EMAIL ADDRESS

5.20.10 Attachment C (References)

RESPONDENT SUBMITTING PROPOSAL: Securus Technologies

1. COMPANY NAME:	Arizona Dept of Corrections		
ADDRESS:	1645 W Jefferson Phoenix, Az. 85007		
CONTACT PERSON:	Jeff Stewart		
TELEPHONE:	602-542-3879	E-MAIL ADDRESS	jstewart@azcorrections.gov
2. COMPANY NAME:	Northern Neck Regional Jail		
ADDRESS:	3908 Richmond Rd. Warsaw, VA 22572		
CONTACT PERSON:	Ted Hull		
TELEPHONE:	804-333-6419	E-MAIL ADDRESS	ted@nnrj.state.va.us
3. COMPANY NAME:	Westchester County Department of Corrections		
ADDRESS:	10 PO Box Valhalla, NY 10595		
CONTACT PERSON:	Capt. Mark Reimer		
TELEPHONE:	914-231-1232	E-MAIL ADDRESS	N/A
4. COMPANY NAME:	Suffolk County Department of Corrections		
ADDRESS:	100 Center Drive Riverhead, NY 11901		
CONTACT PERSON:	Warden Charles Ewald		
TELEPHONE:	631-852-2281	E-MAIL ADDRESS	cewald@optonline.net
5. COMPANY NAME:	Rockland County Jail		
ADDRESS:	55 New Hempstead Road New City, NY 11901		
CONTACT PERSON:	Lt. Joseph McDonald		
TELEPHONE:	845-638-5951	E-MAIL ADDRESS	mcdonald@rcpin.net

☒ Securus has read, understands, and complies.

5.20.11 Attachment D (Questionnaire)

1. Please provide a detailed project plan to include the multiple phases contemplated in this RFP.

✓ **Securus has read, understands, and complies.**

Please refer to Appendix A for our Preliminary Project Plan. A more detailed project plan will be provided upon notice of award and after implementation discussions with appointed Maricopa County personnel

2. How would pricing be impacted if the County chooses to expedite or delay portions of the scope or entire phases?

✓ **Securus has read, understands, and complies.**

Pricing will not be affected due to expedites or delays in the scope of work. We would ask that delays be discussed so we can minimize the cost impact they would have on Securus.

3. Please provide the resumes of all assigned project personnel. How does your firm manage your Human Resources across the project? For instance, will the proposed personnel be the same throughout the project?

✓ **Securus has read, understands, and complies.**

Securus will use several teams to meet the initial and ongoing needs of Maricopa County. For the implementation of the system, our project managers and system installers will be engaged to manage the timeline and scope of the project as well as the physical installation. Our goal is to also have the on-site administration team engaged at this point to have them fully trained on the system once it goes live.

Our remote technical support "SWAT" group will be engaged to remotely assist during the system installation and will transition to our account support personnel for the ongoing maintenance needs of the system.

Throughout the implementation project and following life of the agreement, your account support team, locally represented by Darrin Hays, will be engaged to ensure we meet our obligations and exceed your expectations. Mr. Hays will be supported by Sales Engineer Greg Nicholson and Sales Vice President Ron Davis in all matters pertaining to the agreement. By extension, all personnel will be made available to successfully manage the project throughout its life cycle.

4. What types of JMS or EMR systems have you integrated with? Please provide a list of implementations that can be visited that have had a multi-system integration into the kiosk.

✓ **Securus has read, understands, and complies.**

Securus has solid, proven experience with integration and currently integrates with more than 110 vendors worldwide and over 60 independent facility-owned systems and shared databases.

Securus has its own dedicated Integration Department that works exclusively on integrating the various systems and products in the corrections environment. Having this dedicated Integration Department allows Securus to deliver fast and flexible solutions for our customers. Securus' technology is flexible and does not mandate rigid specifications when working with facility-owned systems, JMS, OMS, commissary, vendors, etc. Securus will fully cooperate with Maricopa County to automate the systems.

The most common technologies Securus uses to integrate with your systems include: SOAP Web Services, HTTP, FTP push or pull of files in any textual format, JSON, XML-RPC, and TCP Sockets. All of these methods are performed over a secure connection.

Securus is able to transform your data format for insertion into our platform, negating the need for costly code modifications to your system. Securus integration engineers will consult with Maricopa County's IT department or system provider to determine the best integration strategy and approach for your specific application.

5. How would your system sequester data related to HIPAA and attorney-client communications?

✓ **Securus has read, understands, and complies.**

Attorney visits are managed through a separate database to ensure no recording is permitted and access by personnel is not allowed. Likewise, health-related visits can be managed through this interface to maintain compliance with HIPAA mandates.

6. Please provide the mean time to failure for all proposed system components.

✓ **Securus has read, understands, and complies.**

Because Securus is responsible for maintaining all hardware and software as well as regular upgrades to our system, through our ongoing maintenance we constantly refresh each component, extending and preventing components from realizing their mean time to failure.

7. Please provide a detail of the following:
a. Training plan (both initial and ongoing)

✓ **Securus has read, understands, and complies.**

SVV training covers all features in the agreement with the County. Securus uses our own experienced employees to conduct all training through online instructor-led classes or on-site, one-on-one and classroom training sessions at no cost to you. Standard training includes using both hands-on experience with your data and using instructor demonstrations to ensure each trainee understands all SVV concepts.

Securus training programs enable facility staff to use all features the first day of installation. Since products are Web-based, after a two- to three- hour training session most officers find it easy to maneuver through the features immediately.

In addition to standard training, Securus will work with Maricopa County to customize your online training experience to meet the unique needs of your staff and facility. We offer separate classes focused on different agency functions such as, creative investigations, well-organized live call monitoring, and efficient system administration. Training for product upgrades, new facility staff, or a general refresher course is offered through online instructor-led courses available twice a month throughout the year—*Securus ongoing training ensures your staff always “stays on top” current and newly released SVV features.*

SVV Training Course Modules

Securus is committed to providing your staff with training that will maximize the potential of the features implemented at your facility. Training courses are in a user-friendly, task-oriented format to teach your officers what they need to know to do their job. We present courses in separate modules based on the types of duties officers tend to perform using the SCP inmate telephone system while expressing the unique features of applications.

The following table presents the standard SCP training course modules and associated learning objectives.

SVV Course Modules

Course Module	Objective
Overview and Navigation	<ul style="list-style-type: none"> • User types • Appointment types • Process flow • URL - status bar - webcam • Internet speed - storage term • Three main modules
Appointments	<ul style="list-style-type: none"> • Stop or cancel a session • Change date/time • Change terminal • Live monitor sessions

Course Module	Objective
Administration	<ul style="list-style-type: none"> • Users and user groups • Terminals and locations • Logs
Session Viewer	<ul style="list-style-type: none"> • View a recorded session • Actions and icons - search, play, lock, delete
Visitation Schedule	<ul style="list-style-type: none"> • Customized by user type
Optional Applications	<ul style="list-style-type: none"> • Sick Call - symptoms • Commissary Ordering • Automated inmate information

b. Maintenance plan

✓ **Securus has read, understands, and complies.**

SVVs centralized design allows for system upgrades three to four times a year, at no cost to the County, to prevent obsolescence in your technology, while also providing for facility growth.

Securus will work with the county to establish a maintenance plan that includes quarterly, monthly, and weekly needs assessments.

- **Maintenance Cycle:** Our on-site technicians will be responsible for preventive maintenance, along with following any existing plan the county prefers to proactively check equipment on a regular basis for maintenance issues. This includes test calls to verify proper rating of calls and volume.
- **Replacement Cycle:** As the system is hosted, Securus will automatically release updates quarterly. Equipment is replaced on an as needed basis throughout the contract.

On-site technicians are provided as part of our planned solution to ensure our service response time is in accordance with SLAs. These dedicated support personnel are in addition to our existing service infrastructure in the State of Arizona.

c. Product warranty

✓ **Securus has read, understands, and complies.**

As this is a fully hosted and supported system, we will maintain the system at no cost throughout the term of the contract and as long as Maricopa County is a Securus customer. Securus fully warrants the system and all components for the life of the contract and will maintain and replace any terminals as needed.

d. Level 1, 2, 3 tech support with standard turn around times

✓ **Securus has read, understands, and complies.**

The following defines Securus' response times for Maricopa County Jail.

When a facility calls Securus, the event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a resolution timeline and escalation procedure. In all cases, Technical Support will respond in the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when an entire system fails or multiple housing units are not operational.

Response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides an estimated time of arrival.

A P1 event is escalated to the following groups and persons:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

A Priority 2 (P2) assignment occurs when a system event adversely affects system functionality on an entire housing unit.

Response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides an estimated time of arrival. A P2 event is escalated to the Technical Support Department.

A Priority 3 (P3) assignment occurs when a system event adversely affects a single terminal or multiple terminals.

Response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility when the service issue is resolved; if a dispatch is required, Securus contacts the customer and provides an estimated time of arrival. A P3 event is escalated to the Technical Support Department.

5.20.11 Attachment D (Questionnaire)

Securus can meet this requirement through the on-site technicians that will be assigned to Maricopa County Jail.

- e. Software annual support – what is included? How are updates validated for compatibility? How are they delivered to the system?

✓ **Securus has read, understands, and complies.**

All upgrades to the system, three to four annually, are provided at no cost to Maricopa County. Updates are provided through the existing interface and are tested prior to release.

The SVV architecture is built to implement software upgrades in real time, limiting disruption to service. As new features are generally available, the feature is added to the central processor, making the feature available to all facilities; however, Securus will not turn on the feature unless the County authorizes us to do so. If service has to be disrupted for an upgrade, the upgrade will be conducted between the hours of 11 p.m. and 7 a.m.

Your Territory Manager, Darrin Hays, who is dedicated to your account, will communicate when new features are available and will schedule additional training, if needed.

8. This solicitation is anticipating up to a ten year commitment by the selected supplier. How do you propose to address hardware refreshes throughout the life of the contract?

✓ **Securus has read, understands, and complies.**

As improved hardware models become available, Securus will introduce them to MCSO and discuss their deployment in your facilities. The model proposed is in advance of current market available hardware and will be relevant as well as well-suited for a corrections environment for many years to come. And since it is web-based, we will be able to automatically deploy new features for Maricopa County when they become available.

9. Based upon the multiple phases, at what point do you anticipate this contract becoming revenue positive for the County? What is the proposed revenue share percentage? Will the revenue percentage fluctuate as different phases are implemented?

✓ **Securus has read, understands, and complies.**

Exactly when Maricopa County begins receiving shared revenues from SVV depends on usage of the system by inmates and their friends and families. Securus estimates that Maricopa County will begin receiving revenue beginning the 10th month of the agreement if inmates average 1.5 visitation sessions per inmate per month based on an ADP of 10,800. Securus further estimates that if inmates average one visitation session per inmate per month the County will begin realizing commissions beginning in the 15th month. Securus will work to increase usage to drive an earlier date for this as it is mutually advantageous.

Securus has proposed a tiered commission methodology that increases as paid visitation sessions increase. Commission payments will begin immediately after system costs are paid for. Securus propose the following tiered commission payment methodology:

- 25 percent for an average of one visitation session per inmate per month
- 27 percent for an average of 1.2 visitation sessions per inmate per month
- 29 percent for an average of 1.4 visitation sessions per inmate per month
- 31 percent for an average of 1.6 visitation sessions per inmate per month
- 33 percent for an average of 1.8 visitation sessions per inmate per month
- 35 percent for an average of 2.0 visitation sessions per inmate per month
- And so forth for each incremental increase in visitation sessions per inmate per month

10. What languages does your interface support? How long would it take to integrate additional languages?

✓ **Securus has read, understands, and complies.**

As a default, Securus deploys SVV with English and Spanish, and the system has the capability to support up to four languages at one time. If Maricopa County requires a language not in our system Securus will add it.

11. What type of interface does your system support for Third Party software?

✓ **Securus has read, understands, and complies.**

Securus has solid, proven experience with integration and currently integrates with more than 110 vendors worldwide and over 60 independent facility-owned systems and shared databases.

Securus has its own dedicated Integration Department that works exclusively on integrating the various systems and products in the corrections environment. Having this dedicated Integration Department allows Securus to deliver fast and flexible solutions for our customers. Securus' technology is flexible and does not mandate rigid specifications when working with facility-owned systems, JMS, OMS, commissary, vendors, etc. Securus will fully cooperate with Maricopa County to automate the systems.

The most common technologies Securus uses to integrate with your systems include: SOAP Web Services, HTTP, FTP push or pull of files in any textual format, JSON, XML-RPC, and TCP Sockets. All of these methods are performed over a secure connection.

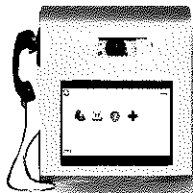
Securus is able to transform your data format for insertion into our platform, negating the need for costly code modifications to your system. Securus integration engineers will consult with Maricopa County's IT department or system provider to determine the best integration strategy and approach for your specific application.

5.20.11 Attachment D (Questionnaire)

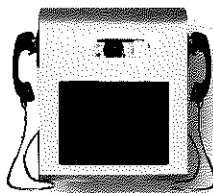
12. Please provide detailed schematics and plans for your proposed kiosk.

✓ **Securus has read, understands, and complies.**

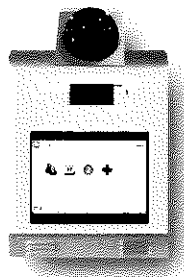
The SVV terminal is constructed as a self-contained, hardened steel case that is wall mounted and equipped with a built-in shatterproof touch screen, a high-resolution video camera with integrated lighting, and a handset for audio communication. However, the tamper-resistant terminals can be mounted in other ways if needed, as shown in the following illustration.



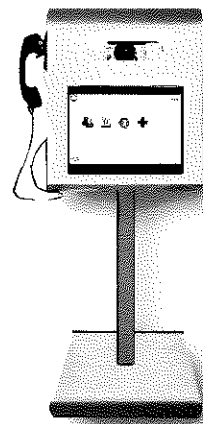
One handset, usually installed inside the housing locations with the inmates.



Two handsets, primarily for visitors.



Hands-free for medical / court / family visits (with PTZ 360° camera).



Units can be mobile or mounted on a pedestal or wall.

The steel braided corrections-grade handset can withstand 1,000 pounds of pressure. Surge protection is implemented on each unit with the ability to maintain clean power in the event of a brown-out, where the voltage drops to 6V. The stations come with a custom mounting bracket that ensures a secure, vandalism-proof installation that also prevents hiding of any contraband within or behind the terminal. On the rear of the station the only cables to connect are power and networking: a 3-prong 120-volt (standard PC power cable) and a CAT6 networking cable. The stations do not require additional cabinetry. All equipment will be approved by MCSO before installation.

13. Regarding security measures, please address the following:

a. What type of Firewalls are being utilized? How many?

✓ **Securus has read, understands, and complies.**

We have a redundant pair of Cisco 5540 firewalls.

5.20.11 Attachment D (Questionnaire)

b. Is there going to be any data encryption technology implemented on this network? What type?

✓ **Securus has read, understands, and complies.**

The video traffic is encrypted via public key/private key RSA encryption. More specifically, 128 bit AES support (session encryption) -RSA public-key cryptography (1024-2048 bit).

c. What type of eMail system is being proposed? Is the data going to be encrypted In/Out?

✓ **Securus has read, understands, and complies.**

Traditionally, facilities provide inmate communications through the telephone and through U.S. Mail. Understanding this, Securus has developed a solution to automate facilities' mail processes and make them safer, more secure, less labor intensive, more visible, more investigative, and even profitable.

Secure Instant Mail enables friends and family members to establish a prepaid email account with Securus to securely send and receive email messages to inmates. These prepaid email transactions **are commissionable, adding an incremental source of revenue to Maricopa County**. Secure Instant Mail was designed to take facilities:

From...	To...
A manual mail process	✓ An automated email process
No revenue related to inmate mail	✓ Increased facility revenue through emails
Limited investigative capabilities	✓ Archived, searchable email database
Potential mailed contraband risks	✓ No mailed contraband physically possible
Labor intensive mail security	✓ Increased security through automation
Limited visibility of inmate mail traffic	✓ Interactive email activity dashboard
Facility staff dedicated to a mail room	✓ Anytime, anywhere email review and approval process from laptops or even smart phones
Standard sort and deliver mail method	✓ Flexible mail options designed to work with facilities' unique needs

Secure Instant Mail also considers the communication needs of inmates' friend and family members in Maricopa County communities, enabling them to:

- Access a simple email interface, designed to look and feel like other public email clients.
- Initiate the communication with the inmate to send and receive emails and even pictures—*anytime, anywhere*.
- Gain peace of mind, knowing the inmate received the mail by viewing approved email delivery receipts.

5.20.11 Attachment D (Questionnaire)

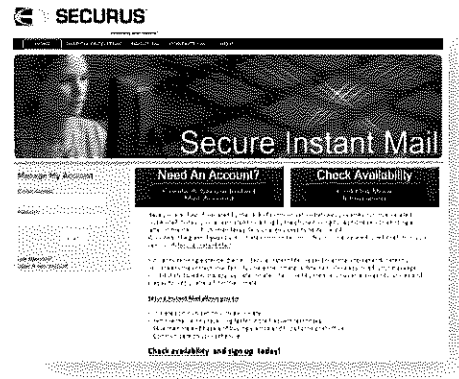
- Communicate more frequently without the need of stamps, envelopes, and on their schedule.

How It Works

Secure Instant Mail is similar to standard email, but built for the corrections environment, meaning it was designed to be flexible, secure, efficient—and profitable.

10. Account Setup and Sending Email

The inmate's friend or family member sets up a Secure Instant Mail account by going to www.securustech.net. Using the Secure Instant Mail website, they can select the facility and inmate receiving the email, compose the email, select messaging options, pay for the email and send the email. Messaging options include requesting approval notifications, prepaying for inmate responses, and even uploading pictures. The email is then processed through the system for the facility's approval before it is sent to the inmate.

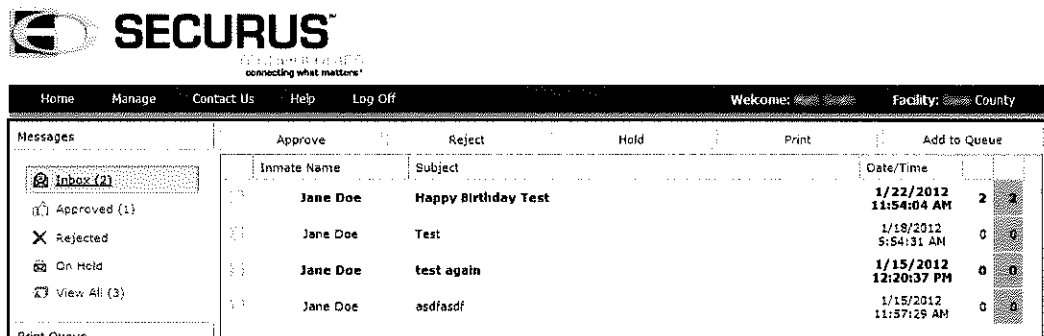


11. Facility Approval

Authorized facility staff logs into the facility's Secure Instant Mail website with a secure user name and password to manage inmate emails. Staff can review, approve, and reject emails and pictures. This process is simplified through a customizable **automatic word search engine**, which flags illicit and potentially illicit words in the emails.

The following figure illustrates the system's capability to flag pending emails that contain word warnings. Their critical relevance is indicated as "red" or "yellow." The facility staff can easily point and click for approval or rejection from any approved PC at anytime, anywhere.

Secure Instant Mail Inbox with Red and Yellow Warning Word Indicator *Proprietary and Confidential*



Once the email is approved, it is archived and can be distributed to the inmate. If the friend or family member has selected to be notified, they would receive an automatic reply email at this time, confirming the approval.

12. Delivery to the Inmate

Maricopa County inmates will receive the email through optional methods including print format and by accessing a Securus Video Visitation kiosk (if available in the facility). Inmates may reply to their email through kiosks or by submitting their written response to facility staff to be approved and scanned into the system to be sent via email to the friend or family member.

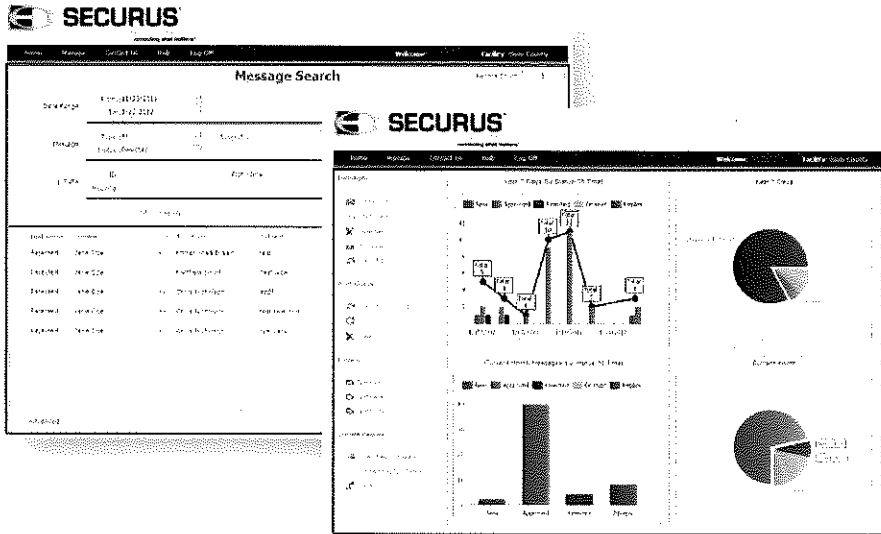
Improving Maricopa County Operations through Automation and Innovation

Secure Instant Mail was not only designed to provide Maricopa County with additional revenue, but also to improve mail room operations security and efficiency. This is accomplished through fully integrated technology that places all automated tools needed to create, approve, send, and receive, and respond to email in the hands of the users.

Secure Instant Mail...

- Eliminates the need to open, analyze, sort, translate, or x-ray mail.
- Reduces contraband, improving the safety of Maricopa County officers as well as inmates.
- Speeds up the emails approval process through integrated word search engine with a built-in, editable dictionary.
- Enhances investigations by archiving each email in a secure centralized database. Through the Secure Instant Mail website, investigators can search for emails by inmate, sender, date range, keyword, and much more.
- Provides an interactive dashboard of email traffic by type, status, and date—giving administrators a complete email management tool right at their fingertips.

Secure Instant Mail Message Search and Interactive Dashboard *Proprietary and Confidential*



14. Although this network environment is primarily being utilized for Web-Based Video Visitation, it will also have to interface with existing systems, forms & databases which currently reside on the Sheriff's Office secured network. With that said, the following items must be addressed as part of the proposals being submitted:

a. What type of virus protection will be implemented on this network?

✓ **Securus has read, understands, and complies.**

Securus installs Symantec AV with current virus definitions on the windows servers.

b. Do you have any plans to utilize Intrusion Detection Systems? (HIDS / NIDS)

✓ **Securus has read, understands, and complies.**

We are not currently using an intrusion detection system, though the firewall allows required access by port filtering.

15. Being that this system will be housing Inmate data & video, it is important that whenever a hard drive fails and requires replacement, the damaged drive **MUST** be turned over to Sheriff's Office Technology Bureau for proper destruction. Will this present issues?

✓ **Securus has read, understands, and complies.**

This does not pertain to our centralized SAN environment. Securus users our centralized data center, not personal computers or other devices with similar hard drives that can fail. However, should a hard drive containing Maricopa County data fail Securus will surrender it to MCSO.

16. In order to make sure that we (MCSO) are always using the latest technology available, a refresh (*The replacement/upgrade of existing technology for the latest version of Hardware/Software [HW/SW]*) of all Desktops; Laptops; Servers; etc. **MUST** take place every 3-5yrs. Since this is a 5yr contract, the expectation would be that the equipment is refreshed, at least once before the end of the contract agreement. Describe this approach:

✓ **Securus has read, understands, and complies.**

To make sure Maricopa County is always using the latest, most up-to-date technologies, Securus upgrades SVV three to four times per year. Additionally, because we maintain the system's components so inmates and their friends and families can conduct video visitation sessions and Maricopa County will earn commission payments, we don't rely on a pre-programmed refresh schedule but replace components should they either fall into disrepair or become obsolete.

17. What if/any is the plan for "Fail-Over" (*Turning off the "Active" server or hard disk and allowing for the "Backup" to take control*) testing; upgrade testing; etc?

✓ **Securus has read, understands, and complies.**

The proposed system uses AT&T MPLS circuits to transport video information from the facility to our disaster resistant data center. Within the AT&T MPLS transport cloud there exists fault tolerance, redundancy, and diversity. This means that in the event of the failure of any individual centralized processor or system within the cloud, sessions are handled by redundant equipment or are rerouted to secondary diverse routes within the overall MPLS network allowing calls to continue to be completed.

Securus SVV was specifically designed to maximize uptime of the platform. Every critical element of the platform has at least one redundant element that operates as a failover in the event of an equipment failure. Additionally, we keep additional pre-programmed equipment spares on hand for each mission-critical element. Finally, our telecom carriers are required to have fully redundant backbone circuitry and our data center is protected by four-hour battery backup, and 36-hour diesel generator protection in the event of a power failure. No inmate telephone provider in the industry can match our level of redundancy or commitment to network uptime.

18. Redundancy is critical...This goes hand-in-hand with "Fail-Over" testing. SW upgrades/updates should be tested on a backup system and upon successful testing, the backup server would become the active server and the active server would then become the backup server. Describe:
- a. RAID 6 on servers
 - b. Redundant Power
 - c. Redundant servers
 - d. "Hot-Swap" Desktops

✓ **Securus has read, understands, and complies.**

The centralized platform is considered highly available and has been designed an engineered so that components are redundant.

Because SVV is a centralized system, records can be accessed by Maricopa County users as if they were stored on-site. To provide protection that effectively lowers the risk of losing data, all data is stored in a centralized database and backed up off site. Our web-based system allows authorized users to access the data from any location with an Internet connection. Securus maintains the system at the highest level of operability.

Securus' SVV provides a unique set of features that use advanced technology to store inmate call recordings. Traditional premises-based calling platforms use local hard drives that may fail and are susceptible to local disasters, such as floods, tornadoes, hurricanes, and fires. The SCP uses storage area network (SAN) storage. SAN is a high-speed sub-network of shared storage devices. SAN's architecture avails all storage devices to all servers on local area networks (LANs) or wide area networks (WANs). Data on the SAN is stored in RAID formats, spreading the data across multiple drives and providing additional protection. Data is no longer susceptible to loss due to an individual drive failure. Accordingly, SANs provide you with the ultimate protection against single drive or server failures as well as increased security for each call recording.

The SVV is co-located in an AT&T Disaster Resistant Carrier Class Data Center that is managed under the direct supervision and immediate hands-on maintenance of highly trained Securus data center personnel.

Visitation session detail and recordings are initially stored for online retrieval on multiple RAID disks in two separate SANs. The system writes all recordings to each SAN, promoting disaster recovery in case of single disk or entire RAID failure.

Off-line archiving is automated and managed by robotic tape drives so you do not have to intervene or archive tape libraries.

19. Please list all sites where your proposed product has been implemented successfully:

✓ **Securus has read, understands, and complies.**

Securus provides the following sites where SVV is installed or in the installation process.

5.20.11 Attachment D (Questionnaire)

Site	State	# of Terminals	Go Live Date	Cut Status
Van Buren	MI	20	12-Aug	Complete
Essex County Jail	NY	5	12-Oct	Complete
Yates County Jail	NY	2	12-Nov	Complete
DeSoto County	MS	24	12-Nov	Complete
Lexington	SC	34	12-Nov	Complete
DeSoto County Expansion	MS	14	3-Dec	Complete
Pottawattamie County	IA	22	4-Dec	Complete
Saline County Jail	KS	32	12/21/2012	Complete
Bibb County	GA	70	1/1/2013	Complete
Migration - Kittitas County Sheriff's Office	WA	27	1/18/2013	Complete
Coos County	NH	1	1/23/2013	Complete
Pulaski County Jail	IN	1	1/23/2013	Complete
Tift County Law Enf. Ct.	GA	13	1/25/2013	Complete
Marion County Jail	FL	107	2/5/2013	Complete
Woodbury County Jail	IA	22	2/12/2013	Complete
Bradley County Jail	TN	30	Onsite Complete At Home TBD	Onsite Complete At Home TBD
Troup County Jail	GA	48	Remote Complete Onsite TBD	Remote Complete Onsite TBD
Montezuma County Jail	CO	11	Complete	Complete



5.20.12 Exhibit 3, Sole Proprietor Waiver (If applicable)

Securus is not a sole proprietor and therefore does not need to submit the Sole Proprietor Waiver.



Addenda Acknowledgements

Securus includes the following Addenda Acknowledgements issued for this RFP:

- Addendum 1
- Addendum 2
- Addendum 3
- Addendum 4

**ATTACHMENT A
PRICING**

SERIAL 13002 - RFP

NIGP CODE: 83834

COMPANY NAME:

Securus Technologies

DOING BUSINESS AS (DBA) NAME:

Securus Technologies

MAILING ADDRESS:

14651 Dallas Parkway, Suite 600

Dallas, TX 75254

REMIT TO ADDRESS:

Same

TELEPHONE NUMBER:

972-277-0300

FACSIMILE NUMBER:

972-277-0514

WEB SITE:

www.securustech.net

REPRESENTATIVE NAME:

Darrin Hays

REPRESENTATIVE PHONE NUMBER:

480-717-8790

REPRESENTATIVE E-MAIL:

dhays@securustech.net

YES NO REBATE

WILL ALLOW OTHER GOVERNMENTAL ENTITIES TO PURCHASE FROM THIS CONTRACT:

X []

WILL ACCEPT PROCUREMENT CARD FOR PAYMENT:

X []

FUEL COMPRISES (if section for fuel price adjustment is located in the solicitation document)

0 % OF TOTAL BID AMOUNT

PAYMENT TERMS: RESPONDENT IS REQUIRED TO PICK ONE OF THE FOLLOWING.

PAYMENT TERMS WILL BE CONSIDERED IN DETERMINING LOW BID. FAILURE TO

CHOOSE PAYMENT TERMS WILL RESULT IN A DEFAULT TO NET 30 DAYS.

[] NET 10 DAYS

[] NET 45 DAYS

[] 1% 10 DAYS NET 30 DAYS

[] NET 15 DAYS

[] NET 60 DAYS

[] 2% 30 DAYS NET 31 DAYS

[] NET 20 DAYS

[] NET 90 DAYS

[] 1% 30 DAYS NET 31 DAYS

[X] NET 30 DAYS

[] 2% 10 DAYS NET 30 DAYS

[] 5% 30 DAYS NET 31 DAYS

1.0 PROFIT SHARING:

1.1 Please provide the rate you charge visitors for one (1) minute of visitation for web usage:

\$0.6475 based on \$12.95 for a 20

1.2 Please provide a anticipated first payment to MCSO post award and implementation:

After system cost paid through se

1.3 Please provide your proposed percentage of profit sharing:

25% for average of one visit per i
27% for average of 1.2 visits per i
29% for average of 1.4 visits per i

ADDITIONAL PRICING

Hourly rates for "out of scope" project personnel

Title	Project Position	Hourly Fee
N/A		

Catalog List Less Percentage Off Discount ***	N/A
---	-----

** *For items not specifically listed on contract